

Cyber-Kriminalität: Nigeria Connection, 0190-Dialer und andere Abzocker

Diplomarbeit

im Fach Informationsnetze, Kommunikationstechnik,
Netzwerkmanagement
Studiengang Informationsmanagement
der
Fachhochschule Stuttgart –
Hochschule der Medien

Miriam Aschenbrenner

Erstprüferin:	Prof. Margarete Payer
Zweitprüfer:	Prof. Askan Blum

Bearbeitungszeitraum: 15. Juli 2002 bis 05. November 2002

Stuttgart, November 2002

Kurzfassung

Die vorliegende Diplomarbeit setzt sich mit der Problematik der Cyber-Kriminalität auseinander. Internet-Kriminalität tritt seit der Geburtsstunde des heute bekannten Internets in zunehmenden Maße auf und hat längst die breite Masse der Internetnutzer als Zielscheibe für Datenmanipulation und -spionage entdeckt. Mit Sicherheitseinstellungen und Vorkehrungen für den sicheren Internetbesuch müssen sich nun verstärkt auch die gelegentlichen Surfer auseinandersetzen. Aus dem weiten Wirkungskreis und den unterschiedlichen Ausprägungsformen von Kriminalität im Internet werden betrügerische Machenschaften vorgestellt, deren Ziel die finanzielle Schädigung der Internetnutzer ist. Abzocker sind Kriminelle im Internet. Anhand zweier Beispiele werden die verschiedenen Methoden von Abzockern näher beleuchtet: Nigeria Connection und 0190-Dialer. Darüber hinaus wird auf die Gefahr bei Internet-Auktionen hingewiesen.

Schlagwörter: Cyber-Kriminalität, Internet-Kriminalität, Nigeria Connection, 0190-Dialer, Internet-Auktion

Abstract

The following dissertation handles the problems of cyber crime. Internet crime has increased since the birth of the Internet and has for sometime targeted the broad mass of Internet users for data manipulation and espionage. The occasional Internet surfer must also now consider the safety adjustment and precautions for safe Internet use. Forms of cyber crime are presented, which aim to damage Internet users financially. Fraudsters are the criminals of the Internet. Two examples show these fraudulent methods: Nigeria Connection and 0190 (premium rate number) Dialer. Additionally the danger of Internet auction is shown.

Keywords: Cyber Crime, Nigeria Connection, 0190-Dialer, Internet fraud, Auction Fraud

Inhaltsverzeichnis

Kurzfassung.....	2
Abstract.....	2
Inhaltsverzeichnis	3
Tabellenverzeichnis	4
1 Einleitung	5
2 Cyber-Kriminalität.....	7
2.1 E-Mail im Internet	10
2.2 Internetnutzung.....	13
3 Nigeria Connection.....	17
3.1 Wahl des Themas	17
3.2 Nigeria – Hintergründe zur Entstehung einer kriminellen Machenschaft.....	18
3.3 Internet in Nigeria.....	24
3.4 Korruption in Nigeria	25
3.4.1 Exkurs: Korruption und Transparency International.....	26
3.5 Vom Brief zur E-Mail	30
3.6 Nigeria Connection, der virtuelle Rachefeldzug Afrikas?!	32
3.7 Untersuchung der Nigeria-Briefe	37
3.8 Fallbeispiele.....	42
3.8.1 Bericht eines thailändischen Geschäftsmanns.....	45
3.9 Rechtliche Strafbelangung.....	47
3.10 Zielgruppe.....	50
3.10.1 Untersuchung der Zielgruppe	51
3.11 Psychologie.....	53
3.12 Verhaltensvorschläge, Kontaktadressen und Maßnahmen.....	54
4 0190-Dialer	57
4.1 Wahl des Themas	57
4.2 0190-Dialer, getarnte Eindringlinge.....	58
4.2.1 Technische Grundlage der Dialer: Trojanische Pferde	58
4.2.2 Vorgehensweise der 0190-Dialer	59
4.3 Fallbeispiel: Opfer der 0190-Abzocke	61
4.4 Rechtliche Strafverfolgung.....	62

4.5	Zielgruppe der 0190-Dialer	64
4.6	Verhaltensvorschläge	66
5	Abzocker.....	70
5.1	Abzocker und Nachahmer des kriminellen Geschäftes	70
6	Zusammenfassung und Ausblick	73
	Anhang A: Ergänzungen zu Themenblock Nigeria Connection	75
A.1	Beispiele für typische Nigeria-Briefe	75
A.2	Liste der Absender der Nigeria-Briefe.....	80
	Anhang B: Adressen und spezielle Informationen für Angeschriebene, Geschädigte und Interessenten.....	82
B.1	Nigeria Connection	82
B.2	0190-Dialer	83
	Literatur- und Quellenverzeichnis	84

Tabellenverzeichnis

Tabelle 1:	Nutzeranteil nach Bevölkerungsgruppen 1997, 1999 und 2001	14
Tabelle 2:	Internetnutzung weltweit, Stand August 2001	15
Tabelle 3:	Erdölförderland Nigeria	20
Tabelle 4:	Überblick wesentlicher Zahlen und Daten von Nigeria	22
Tabelle 5:	Übersicht der technischen Infrastruktur Nigerias	25
Tabelle 6:	Der 2000 Corruption Perceptions Index	29
Tabelle 7:	Vergleich E-Mail-Adressen mit Absender	39
Tabelle 8:	Vergleich Absender mit E-Mail-Adressen	40
Tabelle 9:	Vergleich E-Mail-Adresse und alternative E-Mail-Adresse.....	40
Tabelle 10:	Vergleich übereinstimmender Tel. Nummern	41
Tabelle 11:	Fallentwicklung Computerkriminalität am Beispiel Internetzugangsmissbrauch.....	64

1 Einleitung

„If I were a professional crook, I would do it with computers these days!“ (Fane, zitiert nach Fischer: Computer-Kriminalität, 1979, S. 3). Dieser Ausspruch von Robert Fane, Massachusetts Institute of Technology, aus dem Jahr 1979 oder früher, ist in einer Zeit formuliert worden, in der der Entwicklungsstand der Computerindustrie in den frühen Anfangswehen einer Grundidee des heute bekannten Internets steckte. Dass sich seine Aussage ohne weiteres auf den heutigen Stand des nun existierenden Kommunikationsmittels Internet übertragen lässt, zeigen die verschiedenen Ausprägungsformen der Cyber-Kriminalität. Die vorliegende Diplomarbeit setzt sich mit organisierter Kriminalität im Internet auseinander, dessen Ziel die finanzielle Bereicherung der Betrüger, der Initiatoren der Betrugsformen, ist. Es soll aufgezeigt werden, mit welchen Mitteln, Methoden und Vorgehensweisen die Abzocker arbeiten und welche Internetnutzer bedroht sind. Dabei geht es nicht um technische Grundlagen, sondern vielmehr darum, weshalb sich die betrügerischen Machenschaften erfolgreich im Internet durchsetzen und behaupten können.

Das Kapitel 2 fungiert als Einstieg in das Thema Internet-Kriminalität. Unter der Fragestellung, wie Internet-Kriminalität durch das Internet entstehen konnte, wieviele Internetnutzer als potentielle Opfer unbewusst kandidieren und welche Internetdienste als Tatwaffe eingesetzt werden können, sollen die für die Diplomarbeit ausgewählten Arten der Cyber-Kriminalität definiert werden. Ausgehend von der Grundlage des Kapitels 2 wird die Diplomarbeit in drei weitere Themenblöcke eingeteilt, deren Gewichtung sich in der gewählten Reihenfolge spiegelt: Nigeria Connection, 0190-Dialer und andere Abzocker.

Der Themenblock Nigeria Connection, Kapitel 3, stellt die umfangreichste Abhandlung einer Abzockermasche darstellt. Das Informationsmaterial stellte sich wider Erwarten als äußerst komplex und ergiebig dar, womit die Gewichtung erklärt ist. Das Thema wurde von Prof. Margarete Payer angeregt. Sie ist seit Herbst 2001 Zielscheibe der Nigeria Connection und erhält in zunehmendem Maße Angebotsbriefe von diesen Abzockern. Seit Beantragung des Diplomthemas und der damit beginnenden

¹ Die sinngemäße Übersetzung lautet: Wenn ich ein gewerbsmäßiger Betrüger wäre, würde ich heute mit Computern arbeiten (englisch *crook* = Gauner, Gaunerin).

Auseinandersetzung sind 297 Briefe eingetroffen. Das Kapitel 3.7 beschäftigt sich mit der Untersuchung dieser Briefe. Dabei sind alle Briefe auf gleiche Untersuchungskriterien hin analysiert worden. Interviews mit Fachleuten, ein Erfahrungsbericht eines Betroffenen, einschlägige Pressemitteilungen und Befragungen einzelner betroffener Unternehmen bestimmen den Themenblock Nigeria Connection.

Ein aktuelles und allgegenwärtiges Problem der breiten Internetnutzerschaft wird im zweiten Themenblock, Kapitel 4, behandelt. Die 0190-Abzocker machen sich mit sehr teuren Telefonrechnungen einen Namen. Während der Bearbeitungszeit der Diplomarbeit wurde von der Bundesregierung eine Gesetzesänderung der Telekommunikations-Kundenschutzverordnung verabschiedet. Der inhaltliche Aufbau der Kapitel lehnt sich an den vorausgegangenen Themenblock an. Einschlägige Pressemitteilungen und Auskünfte der Rechtsberatung der IHK Reutlingen bestimmen die Inhalte. Aufgrund der Aktualität war umfangreiches Informationsmaterial über die Presse erhältlich.

Im letzten Themenblock wird auf die Problematik bei Internet-Auktionen hingewiesen (Kapitel 5). Die Diplomarbeit hat auch das Ziel, auf Gefahren im Internet aufmerksam zu machen und die Kehrseite dieses Kommunikationsmittels aufzuzeigen. Die Schattenseite des Internets ist oftmals bekannt, die Verankerung offensiver Schutzmaßnahmen rückt allmählich in das Bewusstsein der Internetnutzer. Mit der Diplomarbeit ist kein Ratgeber oder Wegweiser entstanden, versteckte Appelle dienen der Sensibilisierung für Cyber-Kriminalität. Robert Fane wäre heute vielleicht ein erfolgreicher Abzocker im Internet.

2 Cyber-Kriminalität

Cyber-Kriminalität ist das Produkt des Anfang der 90er Jahre aufblühenden Neuen Mediums Internet. Mit der weltweiten Vernetzung haben sich neben Kommunikations- und Informationsmöglichkeiten auch Formen von Betrugsfällen im virtuellen Raum entwickelt. Der Begriff Cyber-Kriminalität umfasst jede Form von kriminellen Handlungen im Internet, die illegal, organisiert betrügerisch oder menschenrechtsverletzend sind. Die Schlechtigkeiten der realen Welt lassen sich auch im virtuellen Raum umsetzen. Der Online-Betrug boomt und wird technisch gesehen immer raffinierter. Der Begriff Cyber-Kriminalität wird in vorliegender Arbeit als Synonym für Internet-Kriminalität und Cyber Crime gebraucht.

Cyber-Kriminalität = ein Betrug oder Betrugsversuch, der mittels des Tatwerkzeuges eines im Internet angeschlossenen Computers durchgeführt wird. Dabei werden kriminelle, d. h. strafrechtliche Aktionen angewendet. Die Strafhandlung kann eine Einzelperson, aber auch eine Gruppe von Kriminellen ausüben. Man benutzt dabei die verschiedenen Dienste des Internet, z.B. E-Mail und WWW.

Die Schattenseite des Internets heißt Cyber-Kriminalität. Mit der Einführung des heute verwendeten Standard-Internet-Dienst WWW, World Wide Web, fiel auch der Startschuß der Entwicklung von kriminellen Machenschaften. Die Vereinten Nationen von Amerika sind in ihrer Rolle als Vorreiter des Neuen Mediums als erste mit der Problematik der aufkommenden Betrugsformen konfrontiert worden. Das Internet wurde in Amerika entwickelt. Die Auseinandersetzung mit Cyber-Kriminalität spielte anfänglich nur für die amerikanischen Internetnutzer² eine Rolle. Mit der Anpassung an die technische Entwicklung hat sich das Thema Internet-Kriminalität auch in Deutschland und anderen fortschrittlichen Ländern verankert. Das rasche Wachstum der Netze fördert kriminelle Straftaten. Je größer die Nutzerschaft und das Webangebot, desto höher ist die Wahrscheinlichkeit der Ausdehnung von neuen Betrugsformen und deren Opfer. Eine einfache Formel aus der Marktwirtschaft lässt sich gut auf die These übertragen:

² In vorliegender Diplomarbeit wird unter Kenntnisnahme der existierenden weibl. Form nur die männl. Form benutzt. Somit ist mit Internetnutzer auch immer die Internetnutzerin gemeint. Entsprechend gilt dies bei anderen noch auftretenden Begriffen in der männlichen Form.

Angebot und Nachfrage. Ob kriminelle Machenschaften im Internet überhaupt verhindert werden können, ist fraglich (vgl. Schade: Wie mache ich das intelligent?, 1999, S. 3). Durch die hohe Nutzerzahl kann ein einziger Betrüger mehr potentielle Opfer gewinnen als offline. In der Internet-Kriminalität können rund 100 Betroffene auf einen Täter zugeschrieben werden (vgl. Jutzi: Nepper, Schlepper, Surferfänger, 2001, S. 104). Die verbrecherische Entfaltung der phantasievollen Energie von Betrügern findet sich in den vielen Abzockermethoden organisierter Cyber-Kriminalität wieder. Mit einfachen Mitteln werden falsche Tatsachen und Versprechungen vorgetäuscht und die Internet-user zur Kasse gebeten. Das Internet wird als ein vielversprechender und lohnender Tatort entdeckt. Im Jahr 2000 konnte in Deutschland ein Anstieg der Computerkriminalität von 25% verzeichnet werden. Im darauffolgenden Jahr bereits annähernd 40% (vgl. Jutzi: Nepper, Schlepper, Surferfänger, 2001, S. 104).

Die strafrechtliche Verfolgung erweist sich als besonders schwierig, wenn die kriminellen Aktivitäten aus dem Ausland erfolgen. Nationale Grenzen haben im Internet ihre Bedeutung weitgehend verloren. Ab wann z.B. das deutsche Straf- bzw. Ordnungswidrigkeitenrecht Anwendung findet, liegt an der Person oder den Personen, die straf- bzw. ordnungswidrig nach deutschem Recht handeln (vgl. Spindler: Internet-Auktionen, 2001, S. 293). Der Betrugswirkungskreis der Netze ist so groß wie die Netze selbst. Große Probleme in der Internet-Verbrechensbekämpfung bereitet die Identifizierung und Lokalisierung der Gesetzesbrecher. Die Betreiber von Websites mit kriminellen Inhalten stellen diese oft auf ausländische Server. Dadurch soll das Angebot vor dem Zugriff der deutschen Justiz sicher gemacht werden (vgl. Weber: World Wild West, 2000, S. 49).

Die Angebotspalette der verschiedenen Betrugsformen ist vielseitig. Abzocker täuschen Internetnutzer und streichen bei erfolgreicher Umsetzung ihrer Methoden finanzielle Gewinne ein. Cyber-Kriminalität ist nur dann existent, wenn sich immer wieder neue Opfer finden lassen. Es wird nicht auf Formen von Cyber-Kriminalität eingegangen, die unter den Aspekt der Verbreitung von (kinder-)pornografischen Inhalten fallen, dessen Betreiber illegal und menschenrechtsverletzend handeln und dessen Ziel auch eine finanzielle Bereicherung ist. Diese Art von Kriminalität macht zwar einen großen Teil der Betrugsaktivitäten im Internet aus (vgl. Schade: Wie mache ich das intelligent?, 1999, S. 3), kann jedoch im Rahmen der Diplomarbeit nicht behandelt werden.

Eine andere Erscheinungsart von kriminellen Machenschaften sind die Aktivitäten von Hackern. Sie durchsuchen mit Hilfe spezieller Fahndungssoftware die offene Struktur des Netzes nach Sicherheitslücken im Betriebssystem von Rechnern mit dem Ziel, Datenmanipulation, -sabotage und -spionage zu betreiben. Die Motivation von Hackern ist Schäden zu hinterlassen oder wertvolle Informationen und Zahlenmaterial über das Opfer zu erhalten. Eine weitere Motivation ist es, angeblich absolut sichere Systeme auszuhebeln und hierdurch die Verantwortlichen bloßzustellen. Die Frage nach der Sicherheit im Netz und der Gewährleistung durch Vorsichtsmaßnahmen sollten sich insbesondere Unternehmen, Universitäten, Ministerien, Bibliotheken, Banken u. a. stellen, die große und vertrauliche Datenbestände aufweisen. Die zahlreichen elektronischen Attacken auf Zentralrechner in der Vergangenheit belegen diese Notwendigkeit (vgl. Müller von Blumencron: Dämonen im Datennetz, 2000, S. 109).

Zu erwähnen ist auch der virtuelle Schauplatz der Netzpiraten. Der unbefugte und doch sehr gängige Klau von Software-Programmen, PC-Games, MP3-Files, etc. wird durch fehlendes Unrechtsbewusstsein von Seiten der Nutzer und Anbieter praktiziert. Die US-Bundespolizei FBI versucht unter Einsatz von Geboten für die Cyber-Ethik das Rechtsbewusstsein bei der Internet-Nutzung zu stärken: „Du sollst keine Websites verheeren. Du sollst keine Internet-Angebote blockieren. Und du sollst nicht deines Nachbarn MP3-Song begehren“ (NZZ: FBI engagiert sich für Ethik, 2000, S. 53). Die Möglichkeit des E-Mail-Dienstes wird nicht nur für das Versenden von Nachrichten verwendet, sondern auch für Bedrohungen, Erpressungen und Betrug (vgl. Schade: Wie mache ich das intelligent?, 1999, S. 3). Der Themenblock Nigeria Connection (Kap. 3) beschäftigt sich mit dem Betrug durch E-Mail.

Eine Studie in Großbritannien zeigt auf, wie Internetnutzer im Web erfolgreich Betrugsaktionen zum Opfer fallen. Es sind nicht nur die Betrugsversuche der Nigeria Connection und noch nicht die 0190-Dialer, die die Heere der verursachten Schäden entstehen lassen, sondern alltäglicher Handelsbetrug. Der Studie zufolge entstehen die größten Betrugsschäden in Online-Auktionen (vgl. Spiegel: Grand Prix der Webetrüger, 2002, <http://www.spiegel.de/netzwelt/netzkultur/0,1518,197470,00.html>). Die BBC führt eine Liste der 10 am meisten ausgeübten Betrugsarten im Internet auf.

- „ 1. Betrügerische Online-Auktionen, bei der bezahlte Ware nie ausgeliefert wird
2. Die absichtlich falsche Darstellung oder Nicht-Auslieferung online bestellter Konsumgüter (ohne Elektronik)
3. Das beliebte Geldangebot aus Nigeria
4. Die absichtlich falsche Darstellung oder Nicht-Auslieferung von online bestellter Hard- oder Software
5. Betrug mit Zahlungen für den Zugang zu Internet-Diensten: Hier wird kassiert für Dienste, die nie bestellt wurden
6. Die Belastung von Telefonrechnung oder Kreditkarte für Dienste, die entweder nie bestellt, oder aber fälschlich als ‚kostenfrei‘ beworben wurden (häufig geht es um Pornografie)
7. ‚Heimarbeit‘-Angebote mit krass überzeichneten Verkaufs- und Verdienstmöglichkeiten
8. Kreditangebote, bei denen man erst Gebühren zahlt, bevor man keinen Kredit bekommt
9. Kreditkarten-Sonderangebote, die man ebenfalls erst nach Zahlung von Gebühren nicht bekommt
10. Geschäfts- oder Franchisebeteiligungen, die auf Basis bewusst überhöht dargestellter Gewinnaussichten verkauft werden“

(zitiert nach: Spiegel: Grand Prix der Webbetrüger, 2002, <http://www.spiegel.de/netzwelt/netzkultur/0,1518,197470,00.html>). Diese Auflistung dient der Veranschaulichung der verschiedenen Betrugsformen der Cyber-Kriminalität. Im Rahmen der Diplomarbeit werden die Punkte 3. und 6. behandelt, wobei der Schwerpunkt auf der Betrugsform der Nigeria Connection liegt. Internet-Auktionen werden als weitere Abzocker kurz vorgestellt (vgl. Kap. 5.1).

2.1 E-Mail im Internet

Das Internet erhält seine Popularität mit dem Einzug des World Wide Web. Der Zugang zum Internet für private Internetteilnehmer und auch Firmen wird von Providern angeboten. Diese Internetanbieter sehen sich eher als nichtverantwortlich für den Inhalt, der von ihnen weitergegebenen Daten, an. Ein anderer, vielfach genutzter Dienst des Internets ist das Versenden von Nachrichten mittels der elektronischen Post des Internets, der E-Mail. Das komfortable, zuverlässige, preisgünstige und schnelle Kommunikati-

onsmedium ist durch die weltweite Erreichbarkeit von hoher Bedeutung. Das Anlegen einer E-Mail-Adresse bei einem anonymen Mail-Dienst erfordert keine wahrheitsgemäßen Angaben und eignet sich dadurch bestens für kriminelle Absichten.

Die E-Mail ist als Tatwaffe in verschiedenen Ausprägungen einsetzbar. Durch sog. ‚E-Mail-Bombing‘³ können Systeme lahmgelegt werden. E-Mails können zur unaufgeforderten Werbung benutzt werden und die Empfänger belästigen. Durch die Möglichkeit des Anhängens von Attachments mit Viren als auch durch die Inhalte selbst können den Usern Schäden zugefügt werden. Die Zumüllung durch unbrauchbare, unerwünschte und wertlose E-Mails ist nicht nur ein großes Ärgernis der Empfänger, der Speicherplatz und die Zeit werden gestohlen und kann im schlimmsten Fall ebenfalls zum Zusammenbruch des Systems führen. Den höchsten Anteil der unerwünschten E-Mails haben die werblichen Mails. Diese werden als ‚spam‘ bezeichnet und als belästigend empfunden. In Deutschland sind von drei E-Mails zwei unerwünscht (vgl. Test: Nepp mit 0190, 2002, S. 31).

Die Nigeria Connection verwendet den E-Mail-Dienst für organisierten Betrug. Die Verfasser tarnen sich mit fiktiven Namen, und verschicken die Briefe anonym (vgl. Kap. 3.7). Eine Nachricht kann mit einem gefälschten Absender gesendet werden. Re-mailer (spezieller Dienst des Internets) werden ausschließlich dazu verwendet, alle Informationen über den Absender zu verwischen (vgl. Gieseke: Anti-Hacker-Report, 2002, S. 412). Sie kommen daher für die Vorgehensweise der Nigeria Connection nicht in Frage, da die Nigeria-Briefe mit einem Absender versehen sind. Wie werden E-Mail-Adressen gezielt herausgefiltert?

Es ist arglos und leichtgläubig, anzunehmen, dass vertrauliche Informationen im Internet vertraulich bleiben. Der verwendete Webbrowser, der die gewünschten Anfragen beim Webserver abholt, stellt nicht nur die verlangten Websites zur Verfügung, sondern ist mittels des http-Protokolls sehr freigiebig, was Informationen über den Computer und dessen Benutzer anbelangt. Jeder Surfer verrät mehr über sich, als ihm bewusst ist. Der Schutz eigener vertraulicher Daten ist im Internet zwar möglich, wird aber von den meisten Nutzern vernachlässigt oder die Nutzer sind sich darüber nicht im Klaren, dass sie eine potentielle Zielscheibe für Werbestrategien, Spionage oder abzockerische Anschläge darstellen. Sicherheitslücken im Betriebssystem sind Ansatzpunkte für Hacker.

³ Auf einen E-Mail-Server oder an eine E-Mail-Adresse werden innerhalb kürzester Zeit hunderttausende E-Mails geschickt.

Es ist ein Irrglauben, dass private PCs nicht davon betroffen sein können (vgl. Kap. 4.2). Welche Informationen über den Benutzer der Webbrowser an den Server preisgibt, kann unter <http://www.privacy.net/anonymizer> eingesehen werden (vgl. Gieseke: Anti-Hacker-Report, 2002, S. 537).

Das Herausfinden von privaten E-Mail-Adressen ist jedenfalls machbar: Suchmaschinen dienen zum Auffinden von Namen und E-Mail-Adressen. Diese durchstöbern alle Websites, auf denen der Name auftaucht. Diese Methode kann selbstverständlich nur dann angewandt werden, wenn ein Teil der E-Mail-Adresse oder des Namens bekannt ist. Wird kein bestimmter Name gesucht, so kann als Suchbegriff das Zeichen ‚@‘ eingegeben werden. Dies listet dann eine Vielzahl von E-Mail-Adressen auf. Werbeagenturen benutzen diese Möglichkeit, um ihre Werbemails im Massenversand zu verschicken. Die Nigeria Connection kommt zunächst nur an die E-Mail-Adressen, dessen Besitzer in einem öffentlich zugänglichen Verzeichnis auftauchen, z.B. Unternehmen im Handelsregister. Ist dort die E-Mail-Adresse nicht genannt, so kann diese auf der Website aufgeführt sein, die mittels Suchmaschinenrecherche ermittelbar ist.

Das Abtasten der Ziffernfolge einer E-Mail-Adresse ermöglicht das Auflisten nach gewünschten Anfangsbuchstaben. So können alle E-Mail-Adressen, die beispielsweise mit *p* beginnen, aufgelistet und angeschrieben werden. Kriminalität im Internet macht sich u. a. diese Möglichkeit für betrügerische Aktionen zunutze, und erhält auf diese Weise lange Listen mit E-Mail-Adressen (Scott: Network Security the Wild West, 2001, S. 62). Tatsache ist, „dass elektronische Adresslisten inzwischen ebenso gehandelt werden wie die Adressen im richtigen Leben“ (vgl. Gieseke: Anti-Hacker-Report, 2002, S. 538). Werbemails werden mit Sicherheit unter Hilfenahme dieser Adressenlisten verschickt, da sie eine möglichst breit angelegte Empfängerschaft erreichen soll. Die Nigeria Connection bedient sich keiner Verteilerliste, die Zielpersonen werden einzeln angeschrieben. Eine Erklärung könnte sein, dass häufig aufgerufene Websites als Qualitätskriterium gelten⁴. Die Ermittlung dieser Websites erfolgt durch einen Suchmechanismus. Auf diese Weise erhält man E-Mail-Adressen, die auf der entsprechenden Website aufgeführt sind. Es wird eine Liste mit den E-Mail-Adressen erstellt. Generell sollte eine Trennung von privater und geschäftlicher E-Mail-Adresse erfolgen. Die Arbeit mit den unnützen Mails hat man aber in jedem Fall. Die auf der eigenen Homepage veröffentlichte sollte nicht die private E-Mail-Adresse sein. Öffentlich bekannt gegebene

⁴ Diese Überlegung kann nicht belegt werden, es handelt sich um eine spekulative Aussage.

Adressen sollten neutral sein und nichts Näheres über die Person verraten, wie beispielsweise den Heimatort oder die Firmenangehörigkeit (vgl. Gieseke: Anti-Hacker-Report, 2002, S. 497). Die persönliche E-Mail-Adresse sollte daher auch nur denjenigen bekannt sein, die sie von der Person erhalten haben. Das Gegenteil ist nach Betrachtung manch Posteingangs der Fall.

2.2 Internetnutzung

Das Internet bringt die weltweite Vernetzung und den damit verbundenen weltweiten Austausch von Informationen mit sich. Wie stark dieses Kommunikationsmittel genutzt wird und wie sich die Anzahl der Nutzer in den letzten Jahren verändert hat, soll anhand statistischer Tabellenwerte ermittelt werden. Die Zahl der Internetnutzer spiegelt die potentiell gefährdeten Betrugsoffer sowie die erhöhte Wahrscheinlichkeit wider, dass sich darunter kriminelle Abzocker befinden. Internet-Kriminalität kann durch jeden weiteren Nutzer prinzipiell gefördert werden. Es soll lediglich die Entwicklung der Internetnutzung in Deutschland fokussiert werden. Der Umgang der Nutzer mit den Angeboten wird nicht behandelt, obwohl das Thema Internet-Kriminalität diesen Untersuchungsaspekt berücksichtigen müsste. Eine handfeste Analyse der bevorzugten Internetangebote und den meistbesuchten Websites kann einschlägiger Fachliteratur entnommen werden. Im Rahmen der Diplomarbeit wird in den Kapiteln der unterschiedlichen Abzocker auf die entsprechenden Websites näher eingegangen.

In Deutschland leben ca. 82 Millionen Menschen. Fast 40% der Bevölkerung ab 14 Jahren sind Internetnutzer (Stand 2001). Folgende Tabelle macht die Internetentwicklung deutlich.

Tabelle 1: Nutzeranteil nach Bevölkerungsgruppen 1997, 1999 und 2001

	1997		1999		2001	
	in Mio.	in %	in Mio.	in %	in Mio.	in %
Gesamt	4,11	6,5	11,10	17,7	24,77	38,8
Geschlecht						
männlich	3,00	10,0	7,22	23,9	14,71	48,3
weiblich	1,11	3,3	3,89	11,7	10,06	30,1
Alter in Jahren						
14-19	0,29	6,3	1,44	30,0	3,33	67,4
20-29	1,27	13,2	2,89	33,0	5,49	65,5
30-39	1,44	12,4	2,89	24,5	6,05	50,3
40-49	0,74	7,7	2,00	19,6	5,21	49,3
50-59	0,33	3,0	1,55	15,1	3,24	32,2
60 und älter	0,04	0,2	0,33	1,9	1,45	8,1

[Quellen: ARD/ZDF-Online-Studie 1997, ARD/ZDF-Online-Studien 1998-2001. Zitiert nach: Eimeren: ARD/ZDF-Online-Studie, 2002, S. 383]

Die Zahl der Internetnutzer hat sich in den vergangenen 4 Jahren deutlich verändert. Vor allem die Jahre 1998 und 1999 zeigen das verstärkte Interesse an der Einrichtung einer Onlineverbindung. Die Versechsfachung der Internetnutzer lässt sich dadurch erklären, dass das Internet in wesentlich mehr Schichten der Bevölkerung Anwendung findet, als dies zu Beginn Anfang der 90er Jahre der Fall war. Der Zugriff auf wichtige Informationen und die Kommunikation mittels E-Mail sind die Hauptbeweggründe für einen Internetanschluss. 24,77 Mio. Menschen sind im Jahr 2001 online. Mit der Einteilung der Internetnutzer in Altersgruppen wird deutlich, welche Bevölkerungsgruppe zu den potentiell gefährdeten Opfer von kriminellen Internetaktivitäten zählt. In der Bevölkerungsgruppe der 14- bis 29-jährigen verfügen zwei Drittel über einen Internetanschluss (vgl. Eimeren: ARD/ZDF-Online-Studie, 2002, S. 384). Im Zusammenhang mit den 0190-Dialern wird dieser Sachverhalt nochmals aufgegriffen (vgl. Kap. 4.5).

Um die Problematik der Cyber-Kriminalität darzustellen, bedarf es nicht nur einer Betrachtung der Internetnutzung und –entwicklung in der BRD. Dort, wo Internetzugänge existieren, ist auch die Frage nach der Kriminalität präsent. In der vorliegenden

Diplomarbeit konzentrieren sich die einzelnen Schwerpunkte auf Formen des in Deutschland auftretenden Internetbetrugs. Da die betrügerischen Aktivitäten nicht nur

in Deutschland geboren, sondern aus dem Ausland nach Deutschland projiziert werden, sollte ein Überblick über die weltweite Situation der Internetnutzung gegeben werden.

Tabelle 2: Internetnutzung weltweit, Stand August 2001

	Internetnutzer (in Mio.)	Bevölkerungsanteil (in %)
Gesamt	513,43	
Kanada / USA	180,68	58,91
Europa	154,63	19,37
Asien / Pazifik	143,99	4,2
Lateinamerika	25,33	4,95
Afrika	4,15	0,54
Mittlerer Osten	4,65	2,73

[Quelle: NUA: How many online?, 2001, URL: http://www.nua.com/surveys/how_many_online/index.html. Zitiert nach : Afemann: Internet für Entwicklungsländer, 2001, http://www.home.uni-osnabrueck.de/uafemann/Internet_Und_Dritte_Welt/AsienBerlin.htm]

Der Datenverkehr wird ausschließlich über die USA geroutet. Von den 300 Gbit/sec. Übertragungskapazitäten wählen 0,7% des internationalen Internetverkehrs andere Routen (Stand Anfang 2001). Eine Kluft zwischen den Industrie- und Entwicklungsländern lässt sich auch anhand der Menge der Internetnutzer aufzeigen. 93% der User zählen zum reichsten Fünftel der Welt, dagegen gehören 0,2% zum ärmsten Fünftel (vgl. Afemann: Internet für Entwicklungsländer, 2001, http://www.home.uni-osnabrueck.de/uafemann/Internet_Und_Dritte_Welt/AsienBerlin.htm). Um den Zugang zum weltweiten Informationsaustausch und die Teilnahme krimineller Betrugereien von beiden Seiten (Betrüger und Betrogener) zu ermöglichen, sind folgende Grundsätzlichkeiten unabdingbar: Telefon, Computer mit Modem und elektrischer Strom. In Deutschland ist dies grundsätzlich realisierbar. Die folgenden statistischen Angaben werden insbesondere in Hinblick auf das Kapitel Nigeria Connection aufgelistet. Es dient der relationalen Wahrnehmung für die unterschiedlichen technischen Gegebenheiten. 80% der Weltbevölkerung hat kein Telefon. In Afrika sind die Hälfte aller Anschlüsse in den Hauptstädten, in denen nur 10% der Menschen wohnen. Nur 0,76% der afrikanischen Bevölkerung besitzt einen Computer.

Das Stromversorgungsnetz liefert nur 30% des afrikanischen Kontinents den dafür notwendigen Strom (vgl. Afemann: Internet für Entwicklungsländer, 2001, http://www.home.uni-osnabrueck.de/uafemann/Internet_Und_Dritte_Welt/AsienBerlin.htm). Die Behauptung, Internet-Kriminalität sei nur den westlichen Ländern zuzuordnen, da die Voraussetzungen in Entwicklungsländern sehr beschränkt sind, ist falsch. Auch wenn die Zahl der Internetnutzer in armen Ländern sehr gering ist, kann nicht davon ausgegangen werden, dass sich die wenigen keinen kriminellen Aktionen im Internet widmen. Der Betrug der Nigeria Connection beweist dies.

3 Nigeria Connection

„Afrikas Rache kommt virtuell: wie der weisse Mann für den Kolonialismus bestraft wird“ (NZZ: Afrikas Rache, 2002, S. 47).

Nigeria Connection = eine nicht überschaubare und nur annähernd zahlenmäßig schätzbare Gruppe von Kriminellen meist nigerianischer Abstammung, die man sich nicht als straffe Organisation vorstellen darf, sondern eher als ein Geflecht von mehreren Einzelpersonen und Verbündeten, bittet bei ihren Adressaten beim Transfer von sehr hohen Geldbeträgen ins Ausland um Unterstützung.

3.1 Wahl des Themas

Als eine Form von organisierter Kriminalität wird die Nigeria Connection⁵ vorgestellt. Primäres Ziel dieser Verbrecherorganisation ist der finanzielle Gewinn durch Täuschung der Opfer. Es ist eine Betrugsform, deren Machenschaften sich unter journalistischen Aspekten wie einen guten Kriminalroman lesen lassen. Die Nigeria Connection sucht den Kontakt zu den potentiellen Opfern über Angebotsschreiben in Form von Brief, Fax und E-Mail. Es wird nur auf die mit E-Mail verschickten Briefe eingegangen, da Formen von Internet-Kriminalität behandelt werden. Es soll untersucht werden, unter welchen Bedingungen eine Betrugsform wie diese in einem Land wie Nigeria entstehen und bestehen kann. Ein Kapitel beschäftigt sich mit der Frage, weshalb die Nigeria Connection Erfolg hat. Warum lassen sich Menschen auf diese Masche ein? Auf Anregung von Prof. M. Payer ist die vorliegende Diplomarbeit zustande gekommen.

Frau Payer ist seit Herbst 2001 Zielscheibe der Nigeria Connection. In immer stärker auftretendem Maße erhält sie Nigeria-Briefe, die seit April 2002 gesammelt und gespeichert werden. Für die Untersuchung der insgesamt 219 Briefe hat sie mir diese zur

⁵ *Anmerkung:* In Presstexten werden zwei Schreibweisen der Bezeichnung Nigeria Connection verwendet. Dies hängt mit den unterschiedlichen deutschen und englischen Rechtschreibregeln zusammen, Nigeria Connection und Nigeria-Connection. Sie ist auch bekannt unter Lagos-Connection und 419-Connection. In vorliegender Arbeit wird die englische Schreibweise verwendet: Nigeria Connection (englisch *connection* = Verbindung, Zusammenhang).

Verfügung gestellt. In Anhang A.1 befinden sich vier ausgewählte Briefe der Nigeria Connection.

Um einen Überblick der Bekanntheit von der Nigeria Connection zu erhalten, wurde eine Recherche in der Suchmaschine Google⁶ durchgeführt. Die Suchanfrage ergibt 11700 Treffer. Ein ausgewogenes Verhältnis an Pressekurzmeldungen und Online-Artikeln sowie den Warnhinweisen und Verhaltensregeln für Betroffene und den potentiell gefährdeten Briefempfängern reflektiert den Popularitätsgrad der nigerianischen Wirtschaftskriminellen.

3.2 Nigeria – Hintergründe zur Entstehung einer kriminellen Machenschaft

Unter welchen Voraussetzungen kann eine Verbrecherorganisation wie die Nigeria Connection (vgl. Kap. 3.6) entstehen? Hintergrundinformationen über das Land und die Bevölkerung in Nigeria sind daher aufzuzeigen. Angaben über die wirtschaftliche Situation, die politischen Verhältnisse und die Bildung der Bevölkerung tragen dazu bei, das Aufkommen einer betrügerischen Machenschaft, die in zunehmendem Maße angewandt wird, zu begreifen.

Geographie und Ethnien

Der Name Nigeria ist aus dem Fluss Niger abgeleitet. Der Niger und sein Nebenfluss (Benue) teilen das Land in eine Y-artige Darstellung. Die drei großen ethnischen Gruppen haben sich in jenen Achsen angesiedelt: Yoruba (21,3%), Ibo (18%) und Haussa (21,3%). Es existieren noch zahlreiche andere Stämme (39,4%) – je nach Definition 250 bis 434 Ethnien – die jedoch nicht behandelt werden.

Die Y-artige Aufteilung des Landes lässt sich auf die Stämme wie folgt aufteilen: Yoruba im Südwesten, Ibo im Südosten und Haussa im Norden. Während sich im Süden Nigerias durch den Einfall portugiesischer Kaufleute über den Seeweg die Christianisierung Ende des 15. Jh. entwickelte, orientierte sich der Norden weiterhin an eigenen Traditionen und der islamischen Religion. Noch heute spürt man die „herrschende Kluft zwischen dem traditionellen N und dem moderneren S“ (Spiegel Almanach, 1999, S. 405).

⁶ URL:<http://www.google.de>, Zugriff am 2002-09-12

Sprache

Umgeben vom frankophonen Sprachraum (Länder Tschad, Niger, Benin und Kamerun), hat Nigeria, bedingt durch die Eingliederung von einem weiteren Kolonialreich der Briten Mitte des 19. Jh., Englisch als offizielle Amtssprache. Dies wird hauptsächlich in den Städten gesprochen. Die Nigeria Connection nimmt auf englisch den Kontakt zu den ausländischen Unternehmen auf (vgl. Kap. 3.7). Die Sprache des Stammes Haussa (Haussa steht nicht nur für den Stamm, sondern auch für alle Ethnien, die im Haussa-Gebiet leben) wird von der Hälfte der Bevölkerung Nigerias gesprochen und ist mit Yoruba und Ibo seit 1979 als offizielle Landessprache anerkannt (vgl. Harenberg Länderlexikon, 1998, S. 755).

Bevölkerung

Eine genaue Zahl von existierenden Stämmen gibt es nicht. Nach Stahn leben schätzungsweise an die 400 ethnisch unterschiedliche Stammesgruppen in Nigeria. Ebenso vage Vermutungen kann man über die Bevölkerungszahl äußern. Den offiziellen Volkszählungen aus den Jahren 1952, 1963 und 1991 zufolge ergibt sich eine jährliche Zuwachsrate von 2,7%. Im islamischen Norden des Landes herrscht die Polygamie, die u. a. das Bevölkerungswachstum verstärkt. Nigeria ist der bevölkerungsreichste Staat und das am dichtesten besiedelte Gebiet Afrikas (vgl. Stahn: Nigeria, 1995, S. 29). Knapp 40% der Nigerianer lebt in Städten. Nach den Wanderungsbewegungen der Ibo- und Haussa-Stämme in den Süden ergibt sich diese Bevölkerungsverteilung: 35% im Norden, 48% im Süden und 17% im sog. Middle Belt.

Herz des Südens: Lagos

Zentrum des modernen Südens bildet Lagos. Im Südwesten werden die Folgen durch den ehemals starken kolonialen und christlichen Einfluss am deutlichsten erkennbar. Lagos ist Wirtschaftszentrum, Millionenstadt und Quelle der Nigeria Connection. Der Kontrast zwischen den größer werdenden Slums mit zunehmender Arbeitslosen- und Kriminalitätsrate und den gut ausgebauten Verwaltungszentren sowie den exklusiven Residenzen der Regierungsbeamten spiegelt die sozialen Disparitäten wider. Lagos ist die ehemalige Hauptstadt Nigerias. Abuja wird 1991 zur offiziell neuen Hauptstadt ernannt. „Das Landesinnere, auf das keiner der großen Stämme Anspruch erhebt, wurde absichtlich als Standort gewählt, um die Einheit des Vielvölkerstaates zu fördern.“ (Harenberg Länderlexikon, 1998, S. 759). Sie unterbietet Lagos mit den 700.000 Einwohnern um Längen: Lagos zählt ca. 12 Mio. Einwohner. Die Folge der wachsenden Ar-

beitslosigkeit, Landflucht und Militärputsche im Laufe der 80er Jahre sind Schwarzmarktgeschäfte. Lagos wird Welthauptstadt des Betruges (vgl. Thamm: Mafia global, 1998, S. 112). Die westlichen Länder werden mit den Nigeria-Briefen konfrontiert (vgl. Kap. 3.6). In den Anfangsjahren der Aktivitäten der Nigeria Connection ist fast jeder Brief mit Lagos, Nigeria unterzeichnet (mündliche Mitteilung von Klaus Benzenhöfer, Landeskriminalamt Stuttgart vom 2002-09-26).

Der Ölboom

Was zunächst die Landbevölkerung in die Stadt hineinzog, um anschließend die stark überfüllten Elendsviertel noch katastrophaler werden zu lassen, war die Euphorie des 1958 entdeckten Exportmittels Erdöl. Der in den 70er Jahren eingesetzte Exportzweig verdrängte die Agrarwirtschaft. Während der Export der Agrarprodukte drastisch zurückging (in den Jahren 1960-70: 84,5% auf 31,7%), explodierte der Absatz von Erdöl zur selben Zeit. Heute ist es „das wichtigste Wirtschaftsgut Nigerias: Es macht 64% der Staatseinkünfte und 96% der Exporterlöse aus.“ (Harenberg Länderlexikon, 1998, S. 757). Den Hochrechnungen zufolge sind die Reserven im Jahr 2020 erschöpft. Neben Nigeria werden u.a. aus Angola und Kongo sehr ähnliche Angebotsschreiben gesendet (vgl. Kap. 3.6).

Tabelle 3: Erdölförderland Nigeria

Erdölförderung in Afrika

Rang	Land	1000 t
1	Nigeria	101 671
2	Angola	31 025
3	Kongo/Zaire	1 516

[Quelle: Petroleum Economist, zitiert nach: Harenberg Länderlexikon, 1998, S. 757, Stand 1995]

Durch den Rückgang der agrarischen Lebensmittel war auch die eigene Versorgung nicht mehr gewährleistet. Die Lebensmitteleinfuhren mussten unter Berücksichtigung des starken Bevölkerungswachstums erhöht werden. Trotz des Ölbooms liegt die Auslandsverschuldung bei 29 358 Mio. US\$ und Nigeria gehört somit „zu den 20 ärmsten Ländern der Welt und ist zu einem wichtigen Entwicklungshilfeempfänger geworden“ (Stahn: Nigeria, 1995, S. 96). Mit der Ölkrise Ende der siebziger Jahre konnte knapp zehn Jahre später wieder ein Anstieg der Agrarwirtschaft verzeichnet werden.

Bildung und Religion

Sowohl die Islamisierung durch arabische Händler und Geistliche mit Beginn des 11. Jhs., als auch die christliche Missionierung seit 1842 prägen das heutige Schulwesen: im Norden Koranschulen, im Süden von Missionen eröffnete Schulen, die sich am englischen Lehrsystem orientierten. „Als größte Religionsgemeinschaft... wirkt der Islam fast schon wie eine nicht-offizielle Staatsreligion“ (Stahn: Nigeria, 1995, S. 102). Die im Land lebenden Muslime werden auf 50% der Bevölkerung geschätzt. Die Christen tragen mit einem Anteil von 40% (Protestanten 21,4%, Katholiken 9,9% und afrikanische Christen 8,7%) und die Animisten⁷ mit 10% der Bevölkerung bei.

„Die eigentliche zivilisatorische Leistung der Missionierung ist in der Einführung des Schulwesens... zu sehen.“ Schulen wurden vornehmlich aus dem Grund errichtet, um „Bürohilfspersonal, Lehrer und Katechisten heranzubilden“ (Stahn: Nigeria, 1995, S. 103-104). Es existieren heute 133 Universitäten und Hochschulen. Die Einschulungsquote in den Grundschulen beträgt 93%. Diese Quote stieg erst in den letzten Jahren. Der Analphabetismus ist trotz der Einführung der Schulpflicht (6-15 Jahre) erheblich: noch sind 32,7% der Männer, und 52,7% der Frauen schreib- und leseunkundig (vgl. Spiegel Almanach, 1999, S. 16). Auch ist die Ausbreitung von öffentlichen Schulen im Norden (Hausa-Land) weitgehendst unterbunden. Den islamischen Vorstellungen zufolge genügen die Lehren des Korans und das Auswendiglernen der Suren. Die Oberschicht - vor allem aus dem Süden - kommt in den Genuss von universitären Abschlüssen. Das Gefälle zwischen Arm und Reich wird verstärkt: 70,2% der Bevölkerung führen ein Leben unter der internationalen Armutsgrenze (Fischer Weltalmanach, 2002, S. 589).

Um die sozialen, geographischen und wirtschaftlichen Strukturen von Nigeria zu verdeutlichen, wird Deutschland als Vergleichsland in folgender statistischen Auflistung gewählt.

⁷ Animismus = der Glaube an anthropomorph gedachte seelische Mächte, Geister und Anschauung, die die Seele als Lebensprinzip betrachtet

Animist = Vertreter der Lehre des Animismus

[Quelle: Duden: Fremdwörterbuch, 1997]

Tabelle 4: Überblick wesentlicher Zahlen und Daten von Nigeria

	Nigeria	Deutschland
Fläche (in km ²)	923 768	357 022
Urbanisierung (in %)	39,3%	87,1
Bevölkerung (Einw. in Mio.)	123,897	82,057
Bevölkerungsdichte (Einw. Pro km ²)	134,0	229,8
Bevölkerungswachstum (in %)	2,84	0,27
Lebenserwartung		
Männer (in Jahren)	51	73
Frauen (in Jahren)	55	80
Analphabeten		
Männer (in %)	32,7	- ⁸
Frauen (in %)	52,7	-
Wirtschaft		
Bruttoinlandsprodukt (in Mrd. US\$)	32,0	2 099,3
Arbeitslosigkeit (in %)	>30%	9,7
Auslandsverschuldung (in Mio. US\$)	29,358	-
Empfangene Entwicklungshilfe (in Mio. US\$)	192	Geberland
Exportenerlöse (in Mio. US\$)	14 103	511 460

[Quellen: Spiegel Almanach, 1999, S. 403; Fischer Weltalmanach, 2002, S. 590]

Rechtssystem

Das Rechtssystem in dem seit 1960 unabhängigen und 1963 zur Republik erklärten Nigeria, kann nicht als einheitliche Rechtsordnung verstanden werden. Drei Rechtsordnungen sind es, die durch historische Entwicklung, kulturelle Zusammensetzung und Kolonialführung entstanden sind: das britische, das islamische Recht und das Customary Law. Eine Besonderheit stellt das Customary Law dar, ein Naturgesetz, „das ursprüngliche Gewohnheitsrecht der eingesessenen Bevölkerung“ (Stahn: Nigeria, 1995, S. 66). Auch mit dem Rechtssystem wird das Nord-Süd-Gefälle deutlich: das islamische Recht bezieht sich hauptsächlich auf die im Norden lebenden Völker, das britische wird für das gesamte Land geltend gemacht und das Customary Law gilt in seinen verschiedenen Anwendungsformen ebenfalls im ganzen Land. Für das islamische Recht wird

⁸ Analphabeten existieren in Deutschland. In den benutzten Quellen stehen hierzu keine Zahlen und ist in diesem Zusammenhang nicht relevant. Entscheidend ist die prozentuale Anteil der Analphabeten in Nigeria, da untersucht wird, wer als Verfasser der Nigeria-Briefe in Frage kommt.

heute der Begriff Scharia verwendet (vgl. Nashat: Konflikte in Nigeria, 2002, S. 3). Um gegen die Nigeria Connection von deutscher Seite aus zu ermitteln, bedarf es der Zusammenarbeit mit den nigerianischen Behörden (vgl. Kapitel 3.9).

Militärherrschaft und Zivilregierung

Mit der Entkolonialisierung, d. h. der Unabhängigkeit Nigerias, beginnt nach dem gescheiterten Versuch der Demokratie in den Anfangsjahren (bis 1966) die Zeit einer Regionalmacht: Das Militärregime hat das Land von 1966 bis 1979 sowie annähernd ununterbrochen von 1983 bis 1999 unter Kontrolle. Soziale und ethnische Spannungen der muslimischen Hausa und der christlichen Ibo bestärken den Nord-Süd-Gegensatz bis heute. „Das nigerianische Kernproblem besteht darin, daß die politische Dominanz... vom Norden ausgeübt wird, während die ökonomisch aktivsten Bevölkerungsgruppen und die wirtschaftlichen Potentiale primär im Süden angesiedelt sind.“ (Körner: Nigeria, 1999, S 47). Knapp drei Viertel des Militärs besteht aus Hausa. Eine einseitige Parteiergreifung und bewaffnete Konflikte sind die Folge des Nord-Süd-Gefälles.

„Die zivile ‚Erste Republik‘ scheiterte Anfang 1966, weil die Politiker die ökonomische und soziale Entwicklung nicht voranbrachten und das Land durch Korruption, Vetternwirtschaft sowie Mißmanagement in den Ruin trieben und regionale Gegensätze bis an den Rand des Bürgerkrieges verschärften.“ (Körner: Nigeria, 1999, S 47). Nach Jahren der Herrschaft durch die Militärdiktatur (u. a. Sani Abacha 1993-1998) versucht der im Mai 1999 zum Staats- und Regierungschef gewählte Olusegun Obasanjo den Demokratisierungsprozess sowie die Realisierung von Reformen in der jetzigen sog. Dritten Republik (Erste Republik 1960-1965; Zweite Republik 1979-1982) umzusetzen.

Nigeria hat die Wunden der vergangenen Jahrzehnte noch nicht verkraftet. Zu sehr hat sich das Land durch den aufboomedenen Ölexport verführen lassen und die Infrastruktur der Regionen vernachlässigt. Die junge Demokratie steckt noch in den Kinderschuhen. Die größte Herausforderung wird die Bekämpfung der Korruption sein. Die Korruption erklärt den Widerspruch, dass der Großteil der Bevölkerung arm ist und nur einige wenige in Luxus leben. Zwar bekommt das Land durch die Ölquellen hohe Exporterlöse, das Geld versickert jedoch in den Privatschatullen korrupter Staatsdiener und Politiker (vgl. Kap. 3.4).

3.3 Internet in Nigeria

Um das Aufkommen der Nigeria-Briefe mittels des E-Mail-Dienstes zu erklären, sind zunächst die technischen Bedingungen hinsichtlich der Telekommunikation und den Neuen Medien in Nigeria zu untersuchen. Das Internet ist die Voraussetzung, warum der Kontakt über E-Mail entstehen konnte (vgl. Kap. 2.1). Um Rückschlüsse auf die Quelle und die potentiellen Urheber der Nigeria-Briefe ziehen zu können, muss man nicht nur Bildungsstand, Beruf und soziale Stellung beachten (vgl. Kap. 3.2), sondern auch die Verankerung des Internets in der nigerianischen Gesellschaft untersuchen. Unter der Fragestellung „Wer steckt hinter der Nigeria Connection“ soll die gegenwärtige technische Infrastruktur Nigerias erläutert werden.

Unter den vier bevölkerungsreichsten Ländern befindet sich - neben China, Indien und Brasilien - Nigeria. Rund 110 Mio. Rechner⁹, die Internetdienste anbieten, wurden 2001 weltweit verzeichnet. Nur 1% dieser Rechner verteilt sich auf die oben genannten Länder. In diesen Staaten leben ca. 43% der Weltbevölkerung.

In Afrika leben 800 Mio. Menschen, nur 3 Mio. haben Zugang zum Internet¹⁰. Der Anteil beläuft sich für Nigeria im Vergleich zur weltweiten Gesamtzahl auf 0,08% (vgl. Afemann: Internet für Entwicklungsländer, 2001, http://www.home.uni-osnabrueck.de/uafemann/Internet_Und_Dritte_Welt/AsienBerlin.htm). Zugang zum Internet ist nicht zwangsläufig kongruent mit den einzelnen Internetnutzern. Die Zahl der tatsächlichen Nutzer eines einzelnen Internetzugangs kann nicht gesondert erfasst werden. Nachstehende Tabelle lässt erkennen, dass die technische Infrastruktur in Nigeria nur wenigen vorbehalten ist. Für das Versenden der Nigeria-Briefe könnten 0,03% der nigerianischen Bevölkerung zur Verantwortung gezogen werden.

⁹ Mit der Bezeichnung Rechner sind auch Internet-Hosts gemeint.

¹⁰ gerundete Angaben

Tabelle 5: Übersicht der technischen Infrastruktur Nigerias

Nigeria	
Einwohner (in Mio.)	106,4
Städt. Bevölkerung (in Mio.)	42,2
Internetzugänge	100.000
Telefone / 1000 Einwohner	4
PCs / 1000 Einwohner	6
Anteil an Internetnutzern (in %)	0,03

[Quelle: Human Development Report (UNDP) NUA, 2000. Zitiert nach: Afemann: Internet für Entwicklungsländer, 2001, http://www.home.uni-osnabrueck.de/uafemann/Internet_Und_Dritte_Welt/AsienBerlin.htm]

Es ist anzunehmen, dass sich die Anzahl der PCs sowie der Telefonanschlüsse in den Städten verdichtet, da Internetzugänge ausschließlich nur in Großstädten vorhanden sind. Rund 60% der Bevölkerung lebt nicht in den Städten, und hat aufgrund mangelhafter Verlegung der Telefonleitungen durch das Land auch keine Telekommunikationsmöglichkeit. Nur ein kleiner Teil der Gesellschaft kann sich ein Telefon oder einen Computer leisten. Dass Armut und verschiedene Einkommensverhältnisse wenig mit mangelnder und fehlender Technik im Land zu tun haben, sind die Folgen der Machenschaften einer korrupten Minderheit, die das Land regiert und das Geld nicht in soziale Bedürfnisse steckt. Das nächste Kapitel zeigt Formen von Korruption auf. Nigeria ist bekannt für seine korrupte Handlungsweise.

3.4 Korruption in Nigeria

In Nigeria existiert seit langer Zeit die Korruption¹¹ auf vielen Ebenen des politischen, wirtschaftlichen und gesellschaftlichen Lebens. Vor allem in der obersten Schicht ist dies an der Tagesordnung. Schmier-, Bestechungs-, Erpressungsgelder etc. fließen in die Kasse korrupter Staatsbeamter. Die Bereitschaft, konkrete Maßnahmen zur Bekämpfung bzw. Eindämmung der Korruption zu entwickeln, ist nach außen gegenüber der Weltöffentlichkeit zwar vorhanden, das korrupte Geschäft wird jedoch weiterhin betrieben. Präsident Olusegun Obasanjo (seit Ende 1999 im Amt) arbeitet mit schleppendem Erfolg an der Korruptionsbekämpfung.

¹¹ Korruption = Bestechung, Bestechlichkeit, moralischer Verfall

Der erste Ansatz wurde durch die Bildung einer Antikorruptionskommission realisiert. „Ihre zehn Mitglieder unter Vorsitz des pensionierten Richters Akanbi haben seit ihrer Einsetzung im September 2000 das Recht, Unterlagen zu beschlagnahmen, Konten zu prüfen und Hausdurchsuchungen vorzunehmen“ (NZZ: Frontenwechsel, 2001, S. 7). Die Wirkung der Antikorruptionskommission ist jedoch umstritten: Kritiker des Präsidenten sehen dies als Wahlkampagne zur Stärkung seines Rufes an, der „unter einer politischen...Stagnation seit seiner Amtsübernahme gelitten habe“ (NZZ: Frontenwechsel, 2001, S. 7). Zwangspensionierungen zahlreicher korrupter hoher Offiziere, Kabinettsmitglieder, Richter und Staatsanwälte sind von Obasanjo eingeleitet worden (vgl. NZZ: Frontenwechsel, 2001, S. 7).

Der Kampf gegen die Korruption ist ein langwieriges Unterfangen. In Nigeria haben Bestechung, Korruption und Veruntreuung Tradition und werden als unvermeidbares Übel angesehen (vgl. Hirschbiegel: Zauberlösung, 2001, S. 20). Der Untergang der beiden ersten demokratischen Regierungsversuche ist nicht zuletzt auch auf das Aufblühen der Korruption und Vetternwirtschaft zurückzuführen. Militärdiktaturen und demokratische Ansätze haben sich seit der Unabhängigkeit abgewechselt (vgl. Kap. 3.2). Konstant hingegen blieb bei beiden Regierungsansätzen das Anwachsen der Korruption und das Versickern des großen Reichtums des Landes in den Taschen der Eliten. Politische Posten wurden in erster Linie nicht zum Erreichen gesellschaftlicher und wirtschaftlicher Ziele genutzt, „sondern zur Abzweigung umfangreicher öffentlicher Ressourcen für Familien, Clans und Günstlinge mißbraucht“ (Körner: Nigeria, 1999, S. 47). Korrupte Akte begünstigen demnach auch Vorteile für Familienmitglieder.

3.4.1 Exkurs: Korruption und Transparency International

3.4.1.1 Definition von Korruption

Korruption ist „kein Begriff des Strafrechts... vielmehr ein sozialwissenschaftlicher Typusbegriff...“ (Ahlf: Korruption, 1998, S. 5).

Nach Cremer ist Korruption im wesentlichen der Missbrauch eines Amtes. Eine Person, die Amtsperson, erhält ein bestimmtes Amt, einen Amtsposten, die sie mit den vorgegebenen Richtlinien zu erfüllen hat. Werden die für das Amt gestellten Anforderungen verletzt, so sind die sog. Amtsnormen nicht erfüllt. „Der Bruch der Amtsnormen erfolgt bewusst und absichtlich zum eigenen Vorteil des Amtsträgers. Die Vorteile können ... dem Amtsträger direkt oder indirekt zugute kommen“ (Cremer: Korruption begrenzen,

2000, S. 21). Der Begriff Korruption lässt sich nach Meinung Cremers in drei Bereiche missbräuchlichen Verhaltens von Amtsträgern zuordnen: Bestechung, Veruntreuung der dem Amtsträger anvertrauten Mittel und der Nepotismus¹²:

Unter **Bestechung** versteht man eine massive Forderung einer verlangten Leistung (Bestechungsleistung), die der Bestechende mit Geld (Bestechungssumme) einfordert. Dabei handelt es sich um „ein[en] Tausch zwischen zwei Akteuren bzw. zwei Gruppen von Akteuren, dem Bestechenden und dem Bestochenen.“ (Cremer: Korruption begrenzen, 2000, S. 21). Die Bestechungsleistung „kann etwa die Erteilung einer Lizenz oder die Vergabe eines öffentlichen Auftrags an den Bestechenden sein. Der Bestochene ist Amtsträger oder hat eine amtsähnliche Vertrauensstellung. Mit der Gewährung der Bestechungsleistung und der Annahme der Bestechungssumme missbraucht der Amtsträger seine Stellung, bricht also die mit seinem Amt verbundenen Amtsnormen. Der Tausch ist... illegal...“ (Cremer: Korruption begrenzen, 2000, S. 22).

Mit dem Begriff **Veruntreuung** wird jener Betrug verstanden, der durch Unterschlagung von öffentlichen Geldern für die Staatskasse entsteht. Veruntreuung wird demnach Beamten zugeschrieben, die über die „Verwendung des staatlichen Budgets“ (Cremer: Korruption begrenzen, 2000, S. 28) in ihrer Amtshandlung Einfluss üben können. Dieses Delikt wird oftmals von einzelnen Amtsträgern ausgeübt. Um Veruntreuung überhaupt erfolgreich durchführen zu können, bedarf es der gegenseitigen Absprache der in den Ablauf involvierter Amtsträger. Der Ablauf der systematischen Veruntreuung und deren Verselbständigung wird in korrupten Ländern eher als selbstverständlich angesehen (vgl. Hirschbiegel: Zauberlösung, 2001, S. 20).

Von **Nepotismus** spricht man, wenn der Amtsträger seine ihm anvertraute Amtsstellung so ausnutzt, dass er Personen, die entweder „Angehörige seiner Familie, seiner ethnischen Gruppe oder Personen gleicher regionaler Herkunft oder gleicher politischer Ausrichtung“ sind, bevorzugt (Cremer: Korruption begrenzen, 2000, S. 26). „Insbesondere wird von Nepotismus gesprochen, wenn die Amtsstellung missbräuchlich genutzt wird, um den Zugang zu dem Kreis der Amtsträger selbst zu regeln“ (Cremer: Korruption begrenzen, 2000, S. 27).

¹² Nepotismus = Vetternwirtschaft

In Nigeria treten alle drei Formen von Korruption auf: Veruntreuung nigerianischer Staatsgelder aus dem Ölgeschäft, Bestechungen von Beamten und Günstlingswirtschaft auf Regierungsebene (vgl. Kap. 3.6).

3.4.1.2 Transparency International

Um größere Transparenz in oft unklare und verdeckte Abwicklungen politischer und wirtschaftlicher Geschehnisse zu bringen, hat sich im Jahr 1993 „eine Initiative zur Bekämpfung der Korruption in internationalen Geschäftsbeziehungen gegründet: *Transparency International (TI)*.“ (Galtung: Zum Beispiel Korruption, 1994, S. 101). TI versteht sich als „eine gemeinnützige, parteipolitisch unabhängige internationale Bewegung“ (TI: Über TI, 2002, <http://www.transparency.de/html/ueberti.html>). Korruption und Transparenz können gleichgesetzt werden mit verdeckten, betrügerischen und offenen, klar einsichtbaren Systemen und Handlungen. Um die Arbeit nicht nur auf nationaler Ebene durchzuführen, sind heute in über siebenzig Ländern „TI-Ableger“ präsent. Diese leisten die Aufklärungsarbeit vor Ort. Eine der Kernaufgaben von TI ist die Erstellung eines Index (Korruptionsindex CPI). Dieser „ordnet die Länder in einer Rangliste ein, die wiedergibt als wie verbreitet Korruption im öffentlichen Dienst und unter Politikern eingeschätzt wird.“ (TI: Über TI, 2002, <http://www.transparency.de/html/ueberti.html>). Nach Ansicht von TI muss sich die Gesellschaft darüber im Klaren sein, dass Korruption die soziale und wirtschaftliche Entwicklung hemmt, sie die Armut verstärkt und die Demokratie in Gefahr bringt (vgl. TI: Über TI, 2002, <http://www.transparency.de/html/ueberti.html>).

Im folgenden wird ein Auszug des Korruptionsindexes CPI aufgelistet, der in der Voll Darstellung 90 Länder platziert hat. Für die Untersuchung der Nigeria Connection sind neben Nigeria noch weitere afrikanische Länder, die in unmittelbarem Zusammenhang mit den Nigeria-Briefen stehen (vgl. Kap. 3.7) sowie fünf westliche Länder zum Vergleich aufgeführt.

Tabelle 6: Der 2000 Corruption Perceptions Index

Rang der Korruptionsfreiheit ¹³	Land	CPI-Punktwert 2000 (10 = keine Korruption; 1 = völlig korrupt)	Verwendete Untersuchungen (aus unterschiedlichen Jahren)	Standardabweichung (d.h. Streuung der Aussagen; 0 = alle Aussagen stimmen überein)
90	Nigeria	1.2	4	0.6
85	Angola	1.7	3	0.4
80	Uganda	2.3	4	0.6
71	Elfenbeinküste	2.7	4	0.8
65	Burkina Faso	3.0	3	1.0
	Simbabwe	3.0	7	1.5
52	Ghana	3.5	4	0.9
34	Südafrika	5.0	10	0.9
17	Deutschland	7.6	8	0.8
14	USA	7.8	10	0.8
10	Großbritannien	8.7	9	0.6
9	Niederlande	8.9	9	0.6
1	Finnland	10.0	8	0.6

[Quelle: Transparency International, CPI,
<http://www.transparency.de/documents/cpi/2000/cpi2000.de.html>]

Nach dem CPI steht Nigeria an erster Stelle der am korruptest eingestuften Länder. Das Erstellen dieses Korruptionsindex basiert auf Aussagen und Wahrnehmungen von Geschäftsleuten und der Öffentlichkeit (vgl. Transparency International: Über TI, 2002, <http://www.transparency.de/html/ueberti.html>).

In dem korrupten Land etabliert sich eine Verbrecherorganisation, die aus der obersten Ebene hervorgeht: Nigeria Connection. Führende nigerianische Politiker, Beamte und Wirtschaftsvertreter bereichern sich durch die Einnahmen, die sie von den ausländischen Geschädigten einfordern (vgl. Hirschbiegel: Zauberlösung, 2001, S. 20). Durch die korrupten Beamten werden die Machenschaften der Kriminellen der Nigeria Connection unterstützt. Aus den Nigeria-Briefen geht hervor, dass es sich um illegales, veruntreutes nigerianisches Staatsgeld handelt, das vor dem Staat Nigeria geschützt und außer Landes gebracht werden muss.

¹³ Der Rang ist aus der Originaldarstellung übernommen worden.

Den Westeuropäern sind die Vorgehensweisen politischer und wirtschaftlicher Prinzipien in Nigeria geläufig. Das Land benötigt finanzielle Unterstützung aus dem Ausland (vgl. Kap. 3.2). Finanzielle Mittel fließen nach Nigeria, wohlwissend, dass veruntreute nigerianische Staatsgelder in die Privatschatullen von Staatsbediensteten und Politikern gewirtschaftet werden. Die Empfänger der Nigeria-Briefe wissen um die Existenz der versprochenen Millionenbeträge und das veruntreute Staatsgeld (vgl. Körner: Nigeria, 1999, S. 47).

3.5 Vom Brief zur E-Mail

Die in diesem Kapitel benannten Nigeria-Briefe beziehen sich auf die konventionellen Briefe der Nigeria Connection. In der vorliegenden Arbeit wird die Bezeichnung Nigeria-Briefe als Sammelbegriff verwendet.

Betrug aus Nigeria wurde das erste Mal 1973 in den USA registriert. In mehr als 66 Ländern (Stand 1995) versucht die Nigeria Connection auf hochprofessionelle Weise neue Opfer zu gewinnen. Deutschland, Großbritannien, USA, Kanada und Japan stehen seit 1988 auf der Zielscheibe. In den folgenden Jahren werden Rumänien, Polen und Bulgarien weitere Empfängerländer der Nigeria-Briefe (vgl. Thamm: Mafia global, 1998, S. 167). Die Entwicklung der Nigeria-Briefe¹⁴ kongruiert mit dem Aufstieg der technischen Telekommunikationsmöglichkeiten. Dem Brief folgte das Fax und anschließend die E-Mail. Allerdings darf man diese Reihenfolge nicht als bedingte Ablösung des vorangegangenen Übertragungsweg sehen. Briefe und Faxe sind seit der Einführung des E-Mail-Massenversandes deutlich zurückgegangen, ganz eingestellt wurden sie noch nicht. Die Nigeria Connection versucht eine weite Streuung ihrer Angebotsschreiben zu erzielen. Unternehmen ohne Internet-Anbindung werden mit dem konventionellen Brief kontaktiert.

Der Brief aus Nigeria

Der Brief weist sich durch immer wiederkehrende Merkmale aus: er kann durch die von Hand geschriebene Adresse erkannt werden. Das Angebotsschreiben liegt meist als Fotokopie vor, die Briefe werden im Massenversand verschickt (vgl. Henauer: Betrüger-

¹⁴ *Anmerkung:* In diesem Kapitel wird auf die unterschiedliche Formen des Nigeria-Briefes eingegangen. Allgemeine inhaltliche Aspekte können kurz erwähnt werden, diese sind jedoch ausführlich durch die Brief-Analyse in Kap. 3.7 beschrieben.

banden, 2002, <http://www.internet.bap.admin.ch/d/aktuell/warnung/n-betrueger.htm>). Die Kosten für das Versenden an sehr viele Empfänger werden so gering wie möglich gehalten. Nicht nur die Inhalte des Anschreibens enthalten falsche Versprechungen, die Briefe sind z. T. auch mit gefälschten Briefmarken frankiert. Um das Ausmaß der Nigeria-Briefe einzugrenzen und damit die Zahl der Betrugsopfer zu senken, hat die Deutsche Post AG im Mai 2000 mit der nigerianischen Post ein Abkommen getroffen: ein sog. „Memorandum of understanding“ (lateinisch *Memorandum* = Denkschrift, englisch *understanding* = Verstand). Im Briefzentrum der internationalen Post in Frankfurt/Main werden erkannte nigerianische Briefsendungen mit gefälschter Freimachung ausgesondert und vernichtet. Es handelt sich nicht um eine Zensur. Der postalische Anteil der Nigeria-Briefe ist seitdem stark zurückgegangen. Im Jahr 1999 sollen allein in London 600 000 Briefe mit falschen Briefmarken aus dem Verkehr gezogen worden sein, weltweit beläuft sich die Zahl auf 20 Mio. Briefe (vgl. Wolf: Farbe des Geldes, 2000, S. 27). Unternehmen erhalten nun ausschließlich Fax- und E-Mail-Angebotsschreiben. Da sich die Nigeria Connection dem technischen Trend angepasst hat, ist das Ausbleiben der Briefe über den konventionellen Weg als eine Folge des E-Mail-Vorteils erklärt.

Das Fax aus Nigeria

Das Fax unterscheidet sich zum Brief nur hinsichtlich der Überbringungsart. Formale und inhaltliche Unterschiede können im Aufbau und der Darstellung nicht festgestellt werden. Die Qualität ist durch das Versenden einer Fotokopie manchmal beeinträchtigt (Faxausdruck einer Kopie).

Die E-Mail aus Nigeria

Eine ausführliche Untersuchung der E-Mails aus Nigeria ist Hauptbestandteil des Kapitels Nigeria Connection. Die nigerianischen Betrüger wissen den für die interaktive Kommunikation sehr entscheidenden E-Mail-Dienst des www (vgl. Kap. 2.1) für ihre Machenschaften auszunutzen. Die Verbreitung der E-Mails wird meist durch Mail-Dienste wie yahoo, hotmail, lycos, usw. realisiert, bei denen eine Identitätsüberprüfung bei der Anmeldung für ein E-Mail-Postfach nicht stattfindet. Die Anonymität des Absenders ist somit gewährleistet. Die Absender der Nigeria Connection tarnen sich mit fiktiven Namen, z. T. von nigerianischen bekannten Persönlichkeiten (vgl. Kap. 3.6). Dadurch ist das Auffinden der realen Person für die Ermittlungen schwierig.

Ob sich durch die unterschiedlichen Übertragungsmöglichkeiten des Nigeria-Briefes prozentual mehr oder weniger Interessenten auf die Machenschaften der Nigeria Connection eingelassen haben, ist fraglich und wird nicht genauer untersucht. Anhand der Statistik des Bundeskriminalamtes lässt sich nicht erkennen, ob der Kontakt über Brief, Fax oder E-Mail hergestellt wurde. Da die E-Mail weder den Brief noch das Fax abgelöst hat, kann man aus den Zahlen keine Rückschlüsse ziehen. Es ergibt sich eine Grobeinteilung¹⁵ des Nigeria-Briefes in die drei Erscheinungsformen machen; Brief: 1988 bis ca. 1995, Fax: 1994 bis 2000, E-Mail: seit 2000.

Die Kontaktaufnahme zu den Unternehmen läuft entweder über die Postanschrift, die Fax-Nummer oder die E-Mail-Adresse. Woher die Nigeria Connection das Adressen-Material bekommt, ist ungeklärt. Handelsregistrauszüge, Telefon- und Telefaxbücher sowie digitale Telefonverzeichnisse im Internet werden wahrscheinlich verwendet, um die Zielgruppe der Nigeria Connection (vgl. Kap. 3.10) anzuschreiben.

3.6 Nigeria Connection, der virtuelle Rachefeldzug Afrikas?!

Seit 1988 macht die Nigeria Connection mittels dubioser Angebotsbriefe in deutschen Unternehmen auf sich aufmerksam. Das Ziel bzw. die Aufforderung des Absenders an das Unternehmen ist schnell klar: man solle sein Konto für die Überweisung einer mehrstelligen Millionensumme bereit stellen. Bei diesem Geld soll es sich meist um veruntreute nigerianische Staatsgelder handeln, um plötzlich unerwartet hohe Erbschaften, u. a., die aus Schutz vor dem nigerianischen Staat außer Land gebracht werden müssen. Für diesen kleinen Gefallen soll das Unternehmen, das angeblich wegen seiner Kompetenz und Seriosität zufolge ausgewählt worden ist, eine große Entschädigung erhalten: von Gewinnbeteiligungen von bis zu 30% ist die Rede. Es handelt sich bei dem Geld i. d. R. um Beträge zwischen 10 und 50 Millionen US\$. Die Absender geben sich oft als gesellschaftlich hochstehende Persönlichkeiten aus, die sich u. a. als leitende Organe oder hochgestellte Mitarbeiter von Behörden, Ministerien und Banken, Repräsentanten von kirchlichen und sozialen Institutionen oder der erdölverarbeitenden Industrie verstehen. Selbst Prinzen werden als Köder angesetzt, um so überzeugend wie möglich aufzutreten (vgl. Henauer: Betrügerbanden, 2002, <http://www.internet.bap.admin.ch/d/aktuell/warnung/n-betrueger.htm>). Die Briefe

¹⁵ Diese Einteilung ließ sich aus verschiedenen Zeitungsberichten ableiten, und erhebt nicht den Anspruch auf Exaktheit. Sie spiegelt die Häufigkeit des Auftretens wider.

stammen nicht nur aus Nigeria, sondern auch aus anderen afrikanischen Staaten. In den vorliegenden Beispielen handelt es sich angeblich um Familienangehörige des verstorbenen Ex-Diktator Sani Abacha (Nigeria), Ex-Führers Mobutu Sese-Seko (Demokratische Republik Kongo, früher Zaire), Ex-Rebellenführer Jonas Savimbi (Angola) und Ex-Präsidenten Laurent Kabila (Demokratische Republik Kongo, früher Zaire).

Mitarbeiter in höheren Posten, Manager und Direktoren der Nigerian National Petroleum Corporation NNPC, City Trust Bank, der Union Bank Nigeria, Nigerian Liquefied Natural Gas NLNG, Ministry works & houseing [!] Nigeria, Zeinth Bank Nigeria usw geben sich auch als Absender der Nigeria-Briefe aus. Die Namen Martins Onye, Amadi Peters, Philips Duke, Henry Duru, Godwin Emeifiele,... treten im Zusammenhang mit den genannten Unternehmen auf¹⁶. Die Begründungen für den Millionentransfer sind unterschiedlich. Als angebliche Herkunft der Geldmengen werden unterschlagene Firmenvermögen, unverhofft aufgetauchte Familienschätze und angebliche Erbschaften nach plötzlichen Todesfällen genannt. Aktuelle wirtschaftliche und politische Geschehnisse werden als Hintergrundgeschichte in die Bittbriefe mit eingeflochten, um die Glaubwürdigkeit bei den angeschriebenen Opfern zu erhöhen. Im Zusammenhang mit dem Terroranschlag vom 11. September 2001 war u. a. von Bargeld die Rede, das in den Trümmern des World Trade Center gefunden worden sei und auf das niemand einen Anspruch erhoben habe. Ebenso hinterließe ein im Pentagon getöteter Mitarbeiter eine hohe Erbschaft. Während des Afghanistan-Einsatzes hat sich ein angeblicher US-Soldat, der einem Sondereinsatzkommando angehöre, gemeldet. Er habe bei einer Patrouille Rauschgiftgewinne in Höhe von 36 Mio. US\$ entdeckt und benötige nun Unterstützung, um das Geld aus Afghanistan zu schaffen (E-Mail von Kriminaloberkommissar Wolfgang Künkele, Polizeidirektion Reutlingen, vom 2002-08-26).

In den Angebotsschreiben von den Familienangehörigen des ehemaligen nigerianischen Diktators Sani Abacha und des früheren angolischen Rebellenführer Jonas Savimbi ist von hinterlassenen Vermögenswerten die Rede, die aufgrund der umstrittenen Vergangenheit des Verstorbenen außer Landes gebracht werden müssen. Die Methoden, wie Abacha und Savimbi das Land beherrschten, stieß auf große Ablehnung (vgl. Spiegel Almanach, 1999, S. 405). Die Hinterbliebenen sehen daher die Besitztümer in Gefahr. Mit den Briefen versuchen die Familienangehörigen auf Mitleid und Verständnis bei

¹⁶ Im Anhang A.2 ist eine Liste mit den Namen aufgeführt, die als Absender der vorliegenden Nigeria-Briefe eingegangen sind.

den Angeschriebenen zu stoßen. Mit spitzfindiger und zynischer Zunge beschreibt ein Journalist der NZZ Maryam Abacha, die auffällig oft um Unterstützung bittet. „Frau Abacha mag aufmerksamen Zeitgenossen aus drei Gründen bekannt sein: Sie pflegte lange Zeit grosse Mengen von Luxuslimousinen in allen Farben des Regenbogens zu sammeln, sie versuchte einst, 30 mit Dollarnoten vollgestopfte Koffer am nigerianischen Zoll vorbeizuschmuggeln und – ach ja, und sie ist die Witwe des Diktators Sani Abacha, dessen Leben als Gewaltherrscher und hemmungsloser Verschwender vor vier Jahren eine vergiftete Viagra-Tablette beendet haben soll, als er sich gerade an drei indischen Gespielinnen ergötzte. Die E-Mail ... ist ein kleines Meisterwerk in der Kunst des Betrugs. Nach einer rührenden Einleitung über das unerträglich frustrierende Leben in Nigeria nach dem Tod ihres Gatten folgen schnell harte Fakten“ (NZZ: Afrikas Rache, 2002, S. 47). Geht man auf die Bittbriefe von Maryam Abacha ein, so unterstützt man nicht nur ein illegales Geschäft (vgl. Kap. 3.9), sondern steht der despotischen Art und Weise, wie Sani Abacha das Land während seiner Dienstzeit diktiert hat, zumindest nicht ablehnend gegenüber und billigt dessen brutale Vergangenheit. Im Gegensatz zu den Schreiben der Angehörigen fallen die Schreiben der Mitarbeiter der oben genannten Banken, Ministerien, Unternehmen, etc eher nüchtern und einfach aus. Das Anliegen ist schnell geäußert und wird nicht in eine zusätzliche Geschichte gehüllt. Die Verfasser geben sich seriös und geschäftlich (vgl. Zietan: Millionen-Einbahnstraße, 2002, <http://www.spiegel.de/netzwelt/netzkultur/0,1518,186621,00.html>). Die Geldbeträge werden zum Hervorheben, ausgeschrieben in Großbuchstaben, hinter den Zahlenbetrag gestellt. Beispiel: 45 000 000 000 US\$ FOURTY FIVE MILLION UNITED STATES DOLLAR. Nach Henauer liegen Schreiben mit ungerundeten Geldbeträgen vor, beispielsweise von 18,3 oder 32,8 Mio. US\$ ist die Rede. Die Betrüger rechnen dadurch mit einer höheren Glaubwürdigkeit der Beträge (vgl. Henauer: Betrügerbanden, 2002, <http://www.internet.bap.admin.ch/d/aktuell/warnung/n-betrueger.htm>).

Eine andere Taktik ist das Ersuchen nach christlicher Gemeinschaft unter den Staaten. In einem Fall bittet ein frommer Christ der Love of Christ Assembly Nigeria um den Transfer von 11 Mio. US\$. Ein Bombenanschlag auf das Gotteshaus habe den Vorsitzenden der Christengemeinde getötet. Das Gemeindevermögen solle nun aus Schutz vor der korrupten Regierung auf ein ausländisches Konto überwiesen werden.

Die fromme Masche zielt auf die christliche Verbundenheit der Mitmenschen und der Angeschriebene solle die Bitte nicht vor Gott ablehnen. Die Schlusszeilen jenes Briefes sind einmalig¹⁷:

„PLEASE NOTE I WILL BEAR ALL COSTS. I DO NOT NEED ANY MONEY FROM YOU. SHOULD I ASK YOU FOR ANY MONEY IN ADVANCE PLEASE REPORT ME TO FBI OR THE SECURITY SERVICE OF YOUR COUNTRY.

Brother Uwom Oluigbo“ (E-Mail der Nigeria Connection vom 2002-07-24).

Bekundet ein Empfänger der Nigeria-Briefe Interesse, sind die Machenschaften und Betrugsformen der Nigeria Connection vielseitig. Eine Variante ist die Forderung nach der Bankverbindung und Kontonummer sowie Blanko-Geschäftspapiere mit Briefkopf des Unternehmens versehen und fingierte Rechnungsformulare – Scheinrechnungen – mit vorschriftsmäßiger Unterschrift und Stempel des ausländischen Empfängers des Nigeria-Briefes (vgl. Troebbs: Nigeria-Connection, 1995, Kopie aus Archiv). Mit dem Erhalt der geforderten Unterlagen haben die nigerianischen Kriminellen die Lizenz zum Abräumen des Kontos des neuen Geschäftspartners. Andere betrügerische Möglichkeiten entstehen durch die Herausgabe der Geschäftsformulare. Eine offiziell wirkende Einladung aus Deutschland ermöglicht bei der Deutschen Botschaft in Lagos die Erschleichung von Einreisevisa für Drogenkuriere und andere Kriminelle (vgl. Henauer: Betrügerbanden, 2002, <http://www.internet.bap.admin.ch/d/aktuell/warnung/n-betrueger.htm>). Typisch ist, dass im weiteren der Transfer der Millionenbeträge sich durch verschiedenste Schwierigkeiten verzögern soll. Für die Bestechung von Beamten, Notarkosten oder unerwarteten Überweisungsgebühren soll der Angeschriebene eine Vorauszahlung leisten. Die Auszahlung des Millionenbetrages wird wegen angeblichen weiteren Provisions-, Verwaltungs- oder Versicherungsgebühren immer wieder hinausgezögert. Angesichts des greifbar nahen Millionenbetrags leisten die Empfänger der Nigeria-Briefe diese Vorauszahlungen (vgl. Kap. 3.9). „Es sind Fälle bekannt, in denen Ausländer alle ihre verfügbaren Mittel eingesetzt, Kredite aufgenommen und Häuser belehnt hatten, um die Ansinnen der Gangster zu erfüllen und schließlich den erhofften Gewinn einzukassieren. Erst der finanzielle Ruin setzte dem üblen Treiben ein Ende“ (Gerny: Via Lagos, 1994, S. 6). In keinem bisher bekannten Fall hat der versprochene Transfer stattgefunden. Für die Geschäftspartner, die ihr Konto nicht zur Verfügung stellen wollen, bieten die Nigerianer eine ausgefallene Möglichkeit an, das Geld nach

¹⁷ Der vollständige Brief ist in Anhang A.1 abgebildet.

Deutschland zu transferieren. Die Dollarnoten werden zur Tarnung schwarz eingefärbt. Damit keine Einreiseprobleme durch den Zoll entstehen, wird das Geld als Diplomatengepäck¹⁸ deklariert. Für die vorgebliche Entfärbung der Geldscheine liefern die Nigerianer eine Spezialchemikalie mit, die zusätzlich 250 000 US\$ kosten und im voraus bezahlt werden solle. Bei persönlichen Treffen zerbrächen die Nigerianer absichtlich die Flasche, um zu verbergen, dass sich unter der obersten Dollarschicht nur wertloses schwarzes Papier befinde. Die Kosten für den Ersatz der Spezialchemikalie solle der Geschäftspartner übernehmen (vgl. FAZ: BKA warnt, 1995, S. 18).

Der Betrug soll laut einer amerikanischen Finanzberatungsorganisation „den drittgrößten ‚Gewerbe- und Handelszweig‘ in Nigeria darstell[en]“ (NZZ: Afrikas Rache, 2002, S. 47). Die Angebotsschreiben kommen überwiegend aus Nigeria, andere afrikanische Staaten ahmen die Machenschaften der Nigeria Connection nach. Briefe aus Togo, Ghana, Sierra Leone, Südafrika und der Elfenbeinküste sind als Absenderländer bereits registriert. Operationsbasen sind in London, Amsterdam, Berlin und aus dem Ruhrgebiet bekannt (vgl. Polizei Ba-Wü: Warnmeldungen, 2002, http://www.polizei-bw.de/fahndung/warnmeldung/warnmeldungen_nigeria.htm). Zwar gelingt es den Kripo-Beamten immer wieder, Mitglieder der Nigeria Connection zu verhaften, der Kern konnte bisher nicht aufgefunden werden. Die Strukturen innerhalb der Nigeria Connection formieren sich immer wieder neu und sind nicht auf Jahre angelegt (vgl. Stark: Kriminelle Nigerianer, 2000, S. 12). Im Folgenden werden die für die Diplomarbeit zur Verfügung stehenden Nigeria-Briefe analysiert.

¹⁸ Diplomaten- und Konsulargut (Diplomatengepäck): Als Diplomaten- und Konsulargut wird Versandware (Päckchen, Paket) bezeichnet, die bei der Grenzüberschreitung keiner Kontrolle oder Einsicht unterliegen darf. Diese muss entsprechend als Diplomaten- oder Konsulargut gekennzeichnet sein. Eine Befreiung im grenzüberschreitenden Warenverkehr wird nur den Leitern und Mitgliedern der diplomatischen und konsularischen Vertretungen und den in ihrem Haushalt lebenden Familienmitgliedern gestattet (mündliche Mitteilung von Herrn Zwick, Zollamt Reutlingen vom 2002-09-27). Es muss angenommen werden, dass die entsprechenden Befugnisse zum Versenden des schwarz eingefärbten Geldes mit Hilfe korrupter Maßnahmen besorgt werden (vgl. Kap. 3.4).

3.7 Untersuchung der Nigeria-Briefe

Die Frage nach der wahren Identität der Verfasser der Nigeria-Briefe wird unbeantwortet bleiben müssen. Die detektivische Suche nach diesen Personen beschäftigt seit dem Auftauchen des ersten Nigeria-Briefes das Bundeskriminalamt und ist somit auch nicht Gegenstand dieser Diplomarbeit. Die Untersuchung der vorliegenden Nigeria-Briefe soll die Frage beantworten, unter welchen Namen die Verfasser sich ausgeben (wer geben sie vor zu sein?) und ob Zusammenhänge der Namen und des Inhaltes zwischen den einzelnen Nigeria-Briefen erkennbar sind. Anfängliche Vermutungen, dass sich hinter Briefen desselben Inhaltes die gleiche Person verbirgt, können bestätigt werden.

Für die Untersuchung werden nur die mit E-Mail verschickten Nigeria-Briefe ausgewertet. Briefe und Faxe liegen zum Zeitpunkt der Untersuchung nur in jeweils einem Exemplar vor und werden daher nicht analysiert.

Der Untersuchungszeitraum wird auf fünf Monate festgelegt (05. April bis 05. September 02). Insgesamt stehen 219 Nigeria-Briefe zur Verfügung, die alle an die E-Mail-Adresse der Professorin M. Payer geschickt worden waren (vgl. Kap. 1). Während der fünf Monate sind Denkbarekeiten zur Häufigkeit des Eintreffens der Nigeria-Briefe und der Verbindung von wechselnden Namen mit ähnlichem Inhalt aufgestellt worden. Die Briefe sind nach folgenden Kriterien analysiert worden: Name des Absenders, E-Mail-Adresse, Datum, Wochentag, Telefonnummer oder Faxnummer, Reply to-Angabe im Text, Betreff/Subject und Inhalt.

Die Überprüfung der Nigeria-Briefe auf Redundanzen und Zusammenhänge erfolgt in einer einfachen Tabelle. Durch das separate Markieren der einzelnen Spalten können die Zelleninhalte sortiert dargestellt werden. Identische Wörter oder Zahlen werden untereinander aufgelistet. Die Untersuchungskriterien lassen sich nach Header (= elektronischer Briefkopf) und Body (= Inhalt) der E-Mail einteilen; die Ergebnisse werden nach dieser Einteilung präsentiert.

Von: MR:CHARLES MBEBE [mailto:jed1000@mailcity.com]
Gesendet: Mittwoch, 14. August 2002 01:48
An: payer@hdm-stuttgart.de
Betreff: assistance

STRICTLY CONFIDENTIAL & URGENT.

I am Mr, Joseph Edward...

Abbildung 1: Auszug Header und Teilansicht Body eines Nigeria-Briefes

Die Nigeria-Briefe sind durchgängig in englischer Sprache verfasst. Seltene Exemplare in holprigem Deutsch konnten – entgegen Pressemitteilungen - mit der Untersuchung nicht festgestellt werden. Die Verfasser der Nigeria-Briefe geben entweder vor, bekannte afrikanische Persönlichkeiten zu sein (vgl. Auswärtiges Amt: Hinweise Nigeria-Connection, 2002, http://www.auswaertiges-amt.de/www/de/laenderinfos/419_.html) oder die Namen sind frei erfunden. Das Preisgeben der Identität wird selbstverständlich vermieden. Die Gefahr des Aufspürens und der damit verbundenen Strafbelangung ist hoch. Ein Großteil der Nigeria-Briefe wird unter dem Namen von angeblichen Familienmitglieder und engen Vertrauten verstorbener Regierungsführer afrikanischer Staaten verschickt (vgl. Kap. 3.6). Die Teilstrukturen der Familie Abacha und Savimbi können nach Vergleich der Nigeria-Briefe aufgezeigt werden.

Sani Abacha:

sein Bruder Abdulkadir, seine Frau Mariam, sein erster Sohn Habib, sein zweiter Sohn Mohammed, sein Cousin Alhaji Mohammed, sein Neffe Sadiq Mohammed und sein persönlicher Berater Kaloma Alli. Desweiteren liegen Briefe von Isa Bello, dem Arzt von Mariam und ihren Rechtsanwälten George Adams, Usman Attah, Alhaji Baba, Kingsley Ahmed und Musa Abubakar vor.

Jonas Savimbi:

sein Sohn David, seine Tochter Sandra und sein Cousin Joseph.

Der Name des Absenders ist nicht zwingend derselbe wie im Briefinhalt (siehe Abb. 1: E-Mail-Header). Fast alle Nigeria-Briefe werden mit vollem Vor- und Nachname spätestens am Ende des Schreibens versehen. Die höfliche Form des Vorstellens soll eine Art von Vertrauen in die Seriosität des Bittstellenden erzielen. Geschichtliches Hintergrundwissen über Nigeria ist keine zwingende Voraussetzung. Durch die auffällig hohe Anzahl der vermeintlichen Familienangehörigen als Absender ist das Wissen um die politische Methodik des Verstorbenen hilfreich. Somit sind auch korrupte Machenschaften und das damit erwirtschaftete Vermögen erklärt. Das Wissen der westlichen Empfänger über Vorgehensweisen korrupter Führer ist für die Zusammenarbeit mit der Nigeria Connection förderlich und wird sogar vorausgesetzt (vgl. Kap. 3.4). Von den Familienangehörigen erweist sich Maryam Abacha, Witwe Sani Abacha (Nigeria) als aktivste Verfasserin. Auf sie und von ihr in Auftrag gegebene Nigeria-Briefe fallen rund 14% aller gesendeten E-Mails. Insgesamt beziehen sich nur fast die Hälfte der Nigeria-Briefe (48,7%) auf Nigeria selbst. Die Bezeichnung Nigeria Connection ist demnach durch die anfänglichen Briefe aus Nigeria geprägt. Nach 14 Jahren haben sich Nachah-

mer aus Angola, Demokratische Republik Kongo (Zaire), Simbabwe, Sierra Leone, Benin und Südafrika durch ähnliche Maschen einen Namen gemacht (vgl. Kap. 5.1). Briefe aus Togo, Ghana und von der Elfenbeinküste sind in dem Untersuchungszeitraum nicht aufgetaucht (vgl. Polizei Ba-Wü: Warnmeldungen, 2002, http://www.polizei-bw.de/fahndung/warmmeldung/warmmeldungen_nigeria.htm). Anonyme Mail-Dienste werden verwendet: lycos (20,6%), yahoo (13,2%), hotmail (3,3%). Daneben gibt es unbekanntere Mail-Dienste wie z. Bsp. mail (8,2%), rediffmail, africamail,... Die E-Mail-Adresse wird öfters aus der Zusammenstellung Name und Zahl@Domain-Name.com gebildet; z. Bsp. : jos_edw04@mail.com, alimusa_4@lycos.com, hajiaa2@hotmail.com, Mammanjos5454@wongfaye.com, usw. Beim Vergleich der E-Mail-Adressen fällt zwar bei keinem der Briefe exakte Übereinstimmung auf, jedoch sind Ähnlichkeiten vorhanden¹⁹.

Tabelle 7: Vergleich E-Mail-Adressen mit Absender

Brief	E-Mail-Adresse	Absender	Datum
1a	bramk@arabia.com	Khumalo, Bram	24. April
1b	bramk_02@arabia.com	Savimbe, Joachim	25. April
2a	jos_edw@mail.com	Edward, Joseph	03. Juni
2b	jos_edw04@mail.com	Savimbi, Sandra	18. Juni

Die Ähnlichkeiten der E-Mail-Adressen 1a+1b sowie 2a+2b erwecken den Anschein, dass sich jeweils derselbe Absender dahinter verbirgt. Die Namen stimmen jedoch nicht überein. Die Überprüfung der Briefinhalte auf Konformität erzielt das Resultat, dass die Briefe 1a, 1b und 2b identisch sind. Die Stichprobe von weiteren Briefen von Sandra Savimbi, Joachim Savimbe und Bram Khumalo lässt erkennen, dass sich am Briefinhalt nichts ändert. Aus dem Vergleich der Briefe 2a und 2b ergeben sich unterschiedliche Staaten, auf die sich die Inhalte beziehen bzw. aus denen die Briefe gesendet wurden. Die Ähnlichkeit der E-Mail-Adressen ist beträchtlich. Es ist anzunehmen, dass die Abkürzung jos_edw für Joseph Edward stehen soll. Die E-Mail-Adresse von Sandra Savimbi weist auf den selben Verfasser, der sich als Joseph Edward ausgibt, hin. Daher kann davon ausgegangen werden, dass es sich bei dem Verfasser der vier Briefe um dieselbe Person oder dieselben Personen handelt. Die im ersten Abschnitt geäußerte

¹⁹ *Anmerkung:* aufgrund von besonders eindeutigen Ähnlichkeiten werden in diesem Zusammenhang Beispiele präsentiert, deren Inhalt sich nicht auf Nigeria, sondern Angola bezieht. Dies dient alleine der Veranschaulichung.

Vermutung der gleichen Urheberschaft kann nun bestätigt werden. Es handelt sich nicht um einen handfesten Beweis, sondern eine sehr wahrscheinliche Annahme.

Absender, die sich wiederholt melden, verwenden ausschließlich unterschiedliche E-Mail-Adressen. Trotz anonymer Mail-Dienste wird dies für eine zusätzliche Tarnung und zum Schutz der eigenen Identität verwendet.

Tabelle 8: Vergleich Absender mit E-Mail-Adressen

Brief	Absender	E-Mail-Adresse	Datum
1	Kabila, Laurent Mpeti	mpet_k@arabia.com	29. April
2	Kabila, Laurent Mpeti	mpeti_k08@mail.com	04. Mai
3	Kabila, Laurent Mpeti	mpeti_k@mail.com	14. Mai

Eine andere Möglichkeit ist der Hinweis einer Reply to E-Mail-Adresse am Briefende. So wird der Kontakt mit einem anderen Mail-Dienst fortgeführt. Diese Möglichkeit weisen 39,2% der Briefe auf.

Tabelle 9: Vergleich E-Mail-Adresse und alternative E-Mail-Adresse

Absender	E-Mail-Adresse	Reply to
Musa, Ali	alimusa_4@lycos.com	ali90@wongfaye.com

Eine Regelmäßigkeit in der Häufung der Nigeria-Briefe kann weder generell noch bei wiederkehrenden Briefen (entweder des gleichen Absenders oder des gleichen Briefinhaltes) festgestellt werden. Entgegen des ersten Eindrucks, die Nigeria-Briefe werden verstärkt zum Wochenende hin und am Wochenende selbst verschickt, zeichnet sich der Mittwoch (17,3%) als der am häufigsten genutzte Tag zum Versenden der E-Mails ab. Dienstag und Freitag sind mit je 16,5% auch stark belastet.

Um die Aufmerksamkeit der Empfänger auf den Nigeria-Brief zu lenken, werden in der Betreff- oder Subject-Zeile häufig drei Begriffe benutzt, die entweder separat oder mit einem verstärkenden Zusatzwort versehen sind: Assistance 20,6% (englisch *assistance* = Beistand, Unterstützung), Business 19,0% (englisch *business* = Beruf, Tätigkeit) und Attention 4,2% (englisch *attention* = Aufmerksamkeit). Zusatzwörter sind u. a. urgent 23,1% (englisch *urgent* = dringend), confidential 13,2% (englisch *confidential* = vertraulich, geheim), proposal 13,2% (englisch *proposal* = Vorschlag). Für die Unterstreichung der Aussage werden die Briefe in Großbuchstaben verfasst. Diese Funktion wird

in rund 20% der Nigeria-Briefe verwendet. Damit soll mit Nachdruck auf die Wichtigkeit und Bedeutsamkeit hingewiesen werden.

Die Anzahl der übereinstimmenden im Brief angegebenen Telefon- und/oder Faxnummern ist relativ gering. Mit einem gegenteiligen Ergebnis wurde gerechnet: Verfasser des gleichen Inhaltes mit unterschiedlichen Namen achten auf eine wiederholte Ziffernfolge. Nur in einem Fall kann eine Übereinstimmung einer Telefonnummer auf drei Namen verteilt eruiert werden.

Tabelle 10: Vergleich übereinstimmender Tel. Nummern

Brief	Name	Tel. Nr.
1	Bashir, Ali Baba	0031 613 777 023
2	Nkroma, David	0031 613 777 023
3	Taytaie, Johnson	0031 613 777 023

Nach Prüfung der Briefe sind große Ähnlichkeiten nachweisbar. Inhaltlich sind die Briefe 2 + 3 identisch. Als Absenderland werden bei allen Briefen die Niederlande, Amsterdam angegeben. Die Vorwahlnummer 0031 ist die Einwahlnummer von Deutschland nach Holland (den Niederlanden). Amsterdam gilt als eine der Drehscheiben von Mittelsmännern der Nigeria Connection in Europa (vgl. Kap. 3.6). Inhaltlich beziehen sich die beiden Briefe auf Farmer aus Simbabwe. Brief 1 bezieht sich auf Sierra Leone. Alle drei Absender benutzen den Mail-Dienst lycos.com. Wie bereits beim Vergleich ähnlicher E-Mail-Adressen kann nach der Gegenüberstellung der Tel. Nummern schlußfolgernd behauptet werden, dass die Briefe 1-3 denselben Verfasser haben dürften. Erwähnenswert ist der Zeitpunkt, an dem die Briefe abgeschickt worden sind. Brief 1 um 12.40 Uhr, Brief 2 um 12.46 Uhr und Brief 3 um 12.50 Uhr, alle am 12. August 2002. Dass es sich um den selben Verfasser²⁰ handeln könnte, ist sehr wahrscheinlich.

Die Urheber der Nigeria-Briefe beziehen sich demnach nicht nur auf einen Staat, sondern übertragen das Prinzip der Angebotsschreiben auch auf andere Länder. Der Hinweis auf das Absenderland muss nicht zwingend die Herkunft des Verfassers sein. In den Beispielbriefen 1 – 3 nimmt der Autor zu den Ländern Sierra Leone und Simbabwe Stellung. Ob es sich bei den vermeintlichen Nachahmern der Nigeria Connection in

²⁰ Verfasser schließt auch die Möglichkeit von mehreren Personen ein, die die Briefe aufsetzen und unter verschiedenen Namen versenden. Mit Verfasser ist daher die Entstehungsquelle gemeint.

anderen afrikanischen Staaten tatsächlich um Nachahmer handelt, oder ob dies nicht dieselben Personen sein könnten, kann nicht bewiesen werden.

Mögliches Täterprofil der Betrüger der Nigeria Connection

Die kriminalistische Beschreibung der Verfasser der Nigeria-Briefe ist in den vorausgegangenen Kapiteln nur mittelbar angesprochen worden. Es soll rückblickend und durch die einzelnen Kapitel unterstützend ein einfaches Täterprofil der Mitglieder der Nigeria Connection angefertigt werden.

Bezüglich der Urheber der Nigeria Connection kann behauptet werden, dass deren Machenschaften folgenden Menschen zuzurechnen sind. Männlich, gebildet, englisch sprechend, wohnhaft im Süden Nigerias (Lagos), Anbindung zum Internet besitzend, über korrupte Vorgänge Bescheid wissend oder selbst korrupt sein sowie sozial und beruflich höherer Schicht angehörend. Die genannten Eigenschaften beziehen sich auf Täter, die entweder in Nigeria leben oder als Mittelsmänner in europäischen Knotenzentren der Nigeria Connection fungieren. Nach Thamm sind nigerianische Betrüger insbesondere Clans der Yoruba-Stämme zuzuordnen. Kriminelle Nigerianer sind auch in anderen afrikanischen Staaten tätig (vgl. Thamm: Mafia global, 1998, S. 112). Dies könnte auf die Nachahmer der Nigeria Connection zutreffen.

3.8 Fallbeispiele

Dass Nigeria-Briefe²¹ in mehr als 66 Ländern (Stand 1995) – hauptsächlich nordamerikanischen und westeuropäischen – bereits aufgetaucht sind, zeigt ein hohes Maß an Streuung (vgl. Thamm: Mafia global, 1998, S. 167). Der Bekanntheitsgrad wächst, publizistische Arbeit wird von Seiten der Zeitungs- und Zeitschriftenverlage durchgeführt und Warnmeldungen der Polizei und des Bundeskriminalamtes existieren ebenfalls.

Um die Streuung der Briefe nicht nur in Bezug auf geographische Verteilung, sondern auch die unterschiedlichen Zielgruppen der Nigeria Connection (vgl. Kap. 3.10) aufzuzeigen, werden zwei Fallbeispiele beschrieben. Es handelt sich im ersten Fall um ein

²¹ Mit der Bezeichnung Nigeria-Briefe sind sowohl die konventionellen, frankierten Briefumschläge als auch Faxesdrucke und die elektronische Briefnachricht gemeint. Der Einfachheit halber wird dies in dem Sammelbegriff gebündelt. Abweichungen, d. h. unterschiedliche Formen der Briefe werden als solche gekennzeichnet und benannt.

finanziell geschädigtes Opfer und im zweiten Fall um einen Versuch aus Neugierde: eine selbständige Schweizerin aus der Freizeitbranche und ein Journalist aus Hamburg.

Der Journalist Winistörfer schildert den Fall der Schweizerin: Ein von Hand adressierter Brief liegt im Jahr 1994 im Briefkasten der selbständigen Schweizerin. Das aus Luftpostpapier bestehende und mit einer exotischen Briefmarke versehene Kuvert weckt sofort die Aufmerksamkeit der Geschäftsfrau. Ein angeblicher Buchhalter der Nationalen Nigerianischen Erdölgesellschaft (NNPC) aus Lagos wendet sich mit der Bitte an sie, ihm bei einer Transaktion von 28 500 000 US\$ aus Nigeria ins europäische Ausland behilflich zu sein. Der Absender nennt sich Dr. Kayode Omosebi. Er gibt vor, ihre Firma seit Jahren zu kennen und vollstes Vertrauen zu ihr zu haben. Die Erdölgesellschaft stehe bei einigen ausländischen Firmen als Schuldner da. Die Höhe der noch offenen Rechnungen ist jedoch falsch verrechnet worden; die Kosten belaufen sich auf 28,5 Mio. US\$ weniger als ursprünglich festgelegt. Um diesen Betrag nun nicht in die nigerianische Staatskasse wandern, sondern sich diesen selbst zukommen zu lassen, benötige er einen verlässlichen Partner im Ausland: die Geschäftsfrau aus der Schweiz. Die Schweizerin fühlt sich durch die süßholzraspelnden Zeilen des nigerianischen Herrn „auserlesen und geschmeichelt“ (Winistörfer: *Jagd nach Millionen*, 1995, S. 18). Ihr Sohn, ein junger Jurastudent, bekräftigt sie in ihrem Vorhaben und schließlich nimmt sie über Fax Kontakt zu Dr. Omosebi auf. Der Ton wird in seinen Antwortschreiben, die sich nun auffallend häufen, rauer und ermahnt seine neue Geschäftspartnerin, die zwei gewünschten leeren Briefbögen mit Blankounterschrift, zwei fiktive Rechnungen sowie Bankverbindung und Kontonummer ihrer Firma zu schicken. Dr. Omosebi telefoniert sogar in die Schweiz. Der raue, befehlstonartige Umgang wird mit den Worten „God bless you“ wieder beschönigt. Ihr Sohn soll wegen dem bevorstehenden Geldtransfer nach Lagos zur Nigerianischen Zentralbank reisen, die Dokumente dort unterschreiben und im Vorfeld noch schnell die Passnummer angeben, damit der Onkel von Omosebi, der angeblich ein Reisebüro hat, ihm eine offizielle Einladung schicken kann. Mit dieser sei ein Touristenvisum ganz schnell beantragt. Es folgen Dokumente des nigerianischen Finanzministeriums und der Nigerianischen Zentralbank, die bestätigen, dass der Einzahlung von 28,5 Mio. US\$ nichts mehr im Wege stehe. Der Sohn fliegt. Im Handgepäck 28 500 US\$, vier Schweizer Luxusuhren, Qualitätsanzüge, Hemden und Krawatten: kurz vor Abflug gibt Dr. Omosebi diese Instruktion, weil der Staat Nigeria angeblich eine Gebühr von einem Prozent der Transfersumme bei Überweisungen veranschlagt. Die Schweizerin nimmt deshalb einen Kredit über 70 000 SFr auf. Der Sohn ist

in Lagos, erhält nach längerem Warten in dem für ihn reservierten Hotel ein dreiseitiges, farbenfrohes Dokument, aber auch den Hinweis, dass das Geld nicht überwiesen werden könne. Wegen des Kurszerfalls der Lokalwährung seien nicht 28 500, sondern 412 000 US\$ Gebühren fällig. Dieses Mal soll das Geld auf ein Konto in New York eingezahlt werden. Der Sohn nach wie vor von dem großen Geld überzeugt, fliegt zurück nach Zürich und schlägt der Mutter den Verkauf des Hauses in der Schweiz vor. Die ist misstrauisch geworden und schreibt Dr. Omosebi, dass sie erst den ihr versprochenen Millionenbetrag auf ihrem Konto sehen möchte, bevor sie weitere Zahlungen durchführt. Dr. Omosebi reagiert drohend, dass er sich nun einen anderen Geschäftspartner suchen würde. Damit ist die Geschäftsbeziehung zwischen Dr. Kayode Omosebi und der um 60 000 SFr ärmeren Unternehmerin beendet. Ein paar Monate später erhält sie erneut Post aus Nigeria. Ein sog. Dr. Dickson Olu, Angestellter in der Finanzabteilung der nigerianischen Erdölgesellschaft, ist auf der Suche nach einem ausländischen Geschäftspartner, der ihm beim Transfer von 28,5 Mio. US\$ von Nigeria in ein europäisches Land unterstützt. Dieser Dr. Olu hat dieselbe Telefonnummer wie Dr. Omosebi (vgl. Winistörfer: Jagd nach Millionen, 1995, S. 18-21).

Das 2. Beispiel stammt von dem Hamburger Journalist Hirschbiegel, bei dem sich Herr Obiora meldet. Der Inhalt der E-Mail ist etwa folgender: Per E-Mail meldet sich James Obiora, ein Manager der Union Bank of Nigeria bei dem Hamburger Journalisten. Er habe folgendes Problem zu lösen, bei dem ihm der deutsche Journalist helfen könne. Ein Amerikaner habe mit der nigerianischen Ölindustrie Millionen verdient. Jener Herr sei nun völlig unerwartet gestorben, und bisher scheine sich kein einziger Verwandter um seinen Nachlass zu kümmern. Damit nun der Manager Obiora selbst das Geld einstecken könne, brauche er die Hilfe des Journalisten. Er bringt sein Anliegen klar und schnell auf den Punkt: der Journalist solle sich als Erbe ausgeben. Dies liefere alles mit sehr unbürokratischen und unkomplizierten Vorgängen ab, der Lohn für den kleinen Aufwand: 30% der Erbschaft. Der Anspruch auf das Erbe müsse mittels Fragen überprüft werden, die nur ein Verwandter beantworten könne. Obiora bestärkt den Deutschen, das könne er nichts falsch machen... Bereits einen Tag später wird bestätigt, dass er als Erbe in Frage komme. Er wird gebeten, dem Rechtsanwalt Christopher Okolie eine Vollmacht zuzufaxen. Ein Schreiben der Nigerian Security Printing and Minting Co erläutert, dass das Geld auf ein niederländisches Konto überwiesen worden sei. Nun bräuchte der Deutsche nur noch einen Termin mit einem in Amsterdam lebenden Mann

ausmachen, um sich den versprochenen Erbschaftsanteil abzuholen. Beim Telefongespräch erwähnte dieser Mann ganz nebenbei, dass sich eine Bearbeitungsgebühr von 10 000 US\$ angesammelt habe, und diese beim Treffen mitzubringen sei. An dieser Stelle brach Hirschbiegel den Versuch ab, mit den Methoden der Nigeria Connection vertraut zu werden. Der Journalist hatte seine berufliche Neugier decken können (vgl. Hirschbiegel: Zaubерlösung, 2001, S. 20).

3.8.1 Bericht eines thailändischen Geschäftsmanns

Durch ein persönliches Gespräch mit dem thailändischen Geschäftsmann Somsak Wongchoossee kann die Kontaktaufnahme zur Nigeria Connection authentisch nachgezählt werden. Herr Wongchoossee ist erfahren in internationalen Geschäften. Im Jahr 1983 erhält er ein Telex von einem Mitarbeiter der staatlichen Ölgesellschaft Nigeria. Für den Transfer von 80 Mio. US\$ solle der thailändische Geschäftsmann sein Konto zur Verfügung stellen. Als Begründung nennt der Absender berufliche Verpflichtungen: als Staatsdiener erhalte man pro Auftrag Provisionen. Bei dem Millionenbetrag handle es sich um Staatsgeld, das mit Hilfe eines fingierten Rechnungsformulars mit dem entsprechenden Betrag von Herrn Wongchoossee locker gemacht werden könne. Als Dank für seine Unterstützung erhalte er 30% der Gesamtsumme (24 Mio. US\$). Der Geschäftsmann sei wegen seiner Zuverlässigkeit auserwählt worden und genieße daher grösstes Vertrauen des nigerianischen Staatsdieners. Herr Wongchoossee hatte niemals zuvor mit nigerianischen Geschäftspartnern zu tun. Zuerst mißtrauisch auf das Angebotsschreiben, „erkannte ich keine Gefahr und dachte, das ist risikofrei. Was soll mir dabei schon passieren?! Ich lagere das Geld, und behalte meinen Anteil.“ (mündliche Mitteilung von Somsak Wongchoossee vom 2002-10-18). Als Fachmann verlangte er nach ordnungsgemässen Vertragsunterlagen, die mit der Aufforderung der Nennung seiner Kontonummer und Bankverbindung von nigerianischer Seite beantwortet wurden. Herr Wongchoossee bestand auf einem persönlichen Treffen in Thailand, um die Existenz des angeblichen Millionenbetrages zu überprüfen, die Nigerianer verlangten wiederum ein Treffen in Nigeria. Eine Einigung konnte nicht erzielt werden, der Mitarbeiter der Ölgesellschaft machte Herrn Wongchoossee darauf aufmerksam, es handle sich um einen Staatsvertrag, der nicht ohne weiteres gebrochen werden könne, er mache sich dadurch strafbar. Mit einem unverschämten letzten Telex brach der Kontakt ab.

Als international agierender Geschäftsmann weiß Herr Wongchoossee über die wirtschaftlichen und politischen Verhältnisse in Nigeria Bescheid, und wäre nie auf den

Vorschlag, nach Nigeria zu reisen, eingegangen. Der Telex-Austausch fand innerhalb weniger Wochen statt. Ein Telex damals war wesentlich teurer als die heute verwendete Versandform E-Mail. Ein Brief in der Länge einer DIN A4 Seite dauerte ca. 3 Minuten. Ein Telex von Nigeria nach Thailand wurde als Ferngespräch abgerechnet. Die Nigeria-Briefe wurden vor rund 20 Jahren sehr bewusst verschickt, da es sich die Betrüger Geld kosten lassen mussten mit ihren Opfern Kontakt aufzunehmen, was mit E-Mails annähernd hinfällig geworden ist. Die Ausweitung der Zielgruppe kann unter anderem auf die Kostenersparnis zurückgeführt werden. Es werden nun verstärkt unerfahrene Leute angeschrieben, die keine Ahnung von Geschäftsbeziehungen vorweisen (vgl. Kap. 3.10). Die Tatsache, dass nun vermehrt auf die Rechtsanwälte der Absender hingewiesen wird, die größtenteils in Holland sitzen, sollte die Empfänger bedenklich stimmen. „Wenn die doch einen Rechtsanwalt haben, warum übertragen sie ihm dann nicht die Verwaltung des Geldes?“ (Herr Wongchoosee vom 2002-10-18). Neugierde und Interesse weichen der Gier nach dem schnellen Geld. Die Briefe werden nicht genau geprüft und aufmerksam durchgelesen. Laut Herrn Wongchoosee sollte eine Firma mit internationalen Erfahrungen auf den Betrug der Nigeria Connection nicht hereinfallen. „Die Zustände in diesem Land sind doch bekannt“ (Herr Wongchoosee vom 2002-10-18). Durch Titel und Bezug auf Ministerium o. ä. werden die Angeschriebenen zusätzlich geblendet. Wenn sich schon ein (angeblicher) Direktor persönlich bemüht, glauben u. U. mehr an die Richtigkeit des Anliegens. Da diese Abzockermasche bereits mehrere Nachahmer praktizieren (vgl. Kap. 5.1), bestehen offenbar keine Absprachen mehr untereinander, wer wem wie oft geschrieben hat (mündliche Mitteilung von Prof. M. Payer vom 2002-10-18). Dies könnte eine Erklärung für das Überhandnehmen der täglich eintreffenden E-Mails dieser Betrüger sein.

Herr Wongchoosee berichtet außerdem von einem Bekannten in Thailand, der ihn vor kurzem angerufen hat und von einem unglaublichen Geschäftsvertrag mit einem Nigerianer erzählte. „Er ist nach wie vor davon überzeugt, dass er bald Millionär sein wird, und träumt von einem neuen Auto, der Renovierung seines Hauses und anderen Dingen, die man eben mit so viel Geld erfüllt“ (Herr Wongchoosee vom 2002-10-18). Dass dieser Bekannte alles verlor und die Forderungen nach noch mehr Vorauszahlungen ihn nicht davon abhalten können, weiterhin an das große Geld zu glauben, klingt nicht nur nach einem Triumphzug der Nigeria Connection, das ist auch das Machwerk dieser kriminellen Bande. Der Bekannte berichtet von einer Frau, die ihm in Fragen der Vertragsabwicklung mit Nigeria unterstützend zur Seite steht. Um den verlangten Geldbe-

tragen nach Nigeria Folge leisten zu können, bat er die Frau, die Gebühren zur Hälfte zu übernehmen um anschließend den Millionengewinn auch zu teilen. Herr Wongchoosee vermutet hinter der angeblichen Vertrauensperson einen Lockvogel. Dies würde die taktische Vorgehensweise der Nigeria Connection bestätigen, da auch in Deutschland solche Mittelsmänner eingesetzt werden, um organisatorische Tätigkeiten vor Ort umzusetzen und persönliche Treffen zu arrangieren. Verhaftungen in einigen Großstädten Deutschlands bestätigen dies (vgl. Kap. 3.6). Ein Lockvogel im eigenen Land ist vertrauenswürdiger, steht dem Opfer mit Rat zur Seite und beteuert die Seriosität und Kompetenz des nigerianischen Bittbriefes (Herr Wongchoosee vom 2002-10-18). Ob der Bekannte immer noch an den versprochenen Transfer glaubt, kann Herr Wongchoosee mit Stand 2002-10-18 nicht sagen.

3.9 Rechtliche Strafbelangung

Betrugsfälle im Internet nehmen zu (vgl. Kap. 2). Durch die Vernetzung können Kriminelle aus jedem Land mit Internet-Anbindung agieren. Die strafrechtliche Verfolgung obliegt den gesetzlichen Bestimmungen des Landes, in dem die Betrugsaktion durchgeführt und von dort aus gesteuert wird. Die Quelle der Betrugsaktion, d. h. der Standort der Betrüger, kann ermittelt werden. Für die strafrechtliche Belangung muss der Wirkungskreis der geltenden Gesetze geklärt werden.

Der Betrug der Nigeria Connection wird als Vorauszahlungsbetrug bezeichnet (vgl. Auswärtiges Amt: Hinweise Nigeria Connection, 2002, http://www.auswaertiges-amt.de/www/de/laenderinfos/419_html). Vorauszahlungen werden dann getätigt, wenn eine Dienstleistung oder ein Produkt im voraus bezahlt werden muss und die Auslieferung der Bestellung zu einem späteren Zeitpunkt erfolgt. Dabei kann es sich um den Gesamtbetrag des Produktes oder um einen Teil der Kosten handeln. I. d. R. erfolgt eine Anzahlung, die einen Teil der Gesamtkosten abdeckt. In den Angebotsschreiben der Nigeria Connection werden Millionenbeträge vorgetäuscht, die in keinem bisher bekannten Fall transferiert worden sind. Die angeschriebenen Unternehmen (Einzelpersonen,...) tätigen aufgrund Versprechungen die geforderten Zahlungen, in der Annahme, für das vorgestreckte Geld die versprochenen Geldbeträge zu erhalten. Ein Tauschgeschäft, das bisher nur einseitig zugunsten der nigerianischen Abzocker durchgeführt worden ist. Bei Betrug gibt es Betrüger und Betrogene. Die Betroffenen der Nigeria Connection fungieren genau genommen auch als Betrüger: bei den angeblichen Geldbe-

trägen soll es sich meist um veruntreute nigerianische Staatsgelder handeln. Geld, das dem Staat gehört und durch korrupte Mitarbeiter in die falsche Kasse gewirtschaftet wurde (vgl. Kap. 3.4). Die Empfänger der Briefe sollen helfen, das Geld vor der korrupten Oberschicht zu retten. Unternehmen, die sich auf das Geschäft mit der Nigeria Connection einlassen, unterstützen den Betrug am Staat. Schwarzgeld soll auf illegalem Weg ins Ausland geschafft werden. Geschädigte amtieren demnach auch als Betrüger. Ihr Verhalten kann jedoch nicht als rechtliche Straftat bewertet werden. Die Handlungsweise kann mit psychologischen Verhaltensmuster beschrieben werden (vgl. Kap. 3.11).

Das Verschicken der nigerianischen Angebotsbriefe wird nach deutschem Recht als straflose Vorbereitungshandlung beurteilt. Von einer straflosen Vorbereitungshandlung spricht man dann, wenn auf die Vorarbeitsmaßnahme keine kriminelle Tathandlung und –durchführung erfolgt. Beispiel: Der Kauf eines Schraubenziehers gilt dann als straflose Vorbereitungshandlung, wenn er im Sinne des eigentlichen Verwendungszweckes auch als solcher gebraucht wird, d. h. zum Anziehen und Lockern von Schrauben. Wird jedoch dieser als Tatwerkzeug für ein Gewaltverbrechen verwendet, so gilt dies als strafbare Vorbereitungshandlung. Die Verfasser der Nigeria-Briefe sind ohne Kontaktaufnahme des Empfängers nicht strafrechtlich verfolgbar. Im Falle einer Anklage könnte jeder vor Gericht sagen, dass es sich um einen Scherz handeln sollte. Der rechtlichen Wirksamkeit des deutschen Gesetzes gegen die Kriminellen der Nigeria Connection sind Grenzen gesetzt. Da die geforderten Vorauszahlungen an die nigerianischen Kriminellen ausschließlich auf ausländische Konten erfolgt, bedarf es der Unterstützung außerhalb des Wirkungskreises des deutschen Rechts. Justitielle Rechtshilfeersuchen sind erforderlich. Interpol und die Staatsanwaltschaft fungieren auf juristischer Ebene, auf diplomatischer Ebene arbeiten Ministerien und Botschaften (mündliche Mitteilung von Kriminaloberkommissar Wolfram Künkele, Polizeidirektion Reutlingen vom 2002-07-31). Die strafrechtliche Belangung der Mitglieder der Nigeria Connection ist auf die Kooperation der deutschen und nigerianischen Seite angewiesen. Die Ermittlungen Richtung Nigeria stellen sich als sehr schwierig und zeitaufwendig heraus. Nigerianische Behörden reagieren kaum auf die Bitten der deutschen Ermittlungsbehörden, die Straftäter zu ergreifen. Ob staatliche nigerianische Stellen selbst in die Vorfälle verwickelt sind, bleibt spekulativ (vgl. Troebbs: Nigeria-Connection, 1995, Kopie aus Archiv). Fest steht, dass sich in höheren Posten im öffentlichen und staatlichen Sektor die korrupte Oberschicht Nigerias bewegt (vgl. Kap. 3.4). Die schleppende Zusammenarbeit

ließe sich so erklären. Die Verschleierung der eigenen Identität der Mitglieder der Nigeria Connection erschwert die rechtliche Verfolgung. Die nigerianischen Geschäftspartner geben sich mit fiktiven Namen aus. Bei den in den Briefen aufgeführten Kontakttelefonnummern (vgl. Kap. 3.7) handelt es sich ausschließlich um prepaid-Mobilnummern. Eine Anschlussinhaberfeststellung ist daher nicht möglich (mündliche Mitteilung von Kriminaloberkommissar Wolfram Künkele, Polizeidirektion Reutlingen, vom 2002-07-31). Gegen die Nigeria Connection erstattet nur ein Bruchteil der Geschädigten Anzeige. Die Scham, auf die Machenschaften hereingefallen zu sein, ist groß und wird deshalb lieber verschwiegen als preisgegeben (vgl. Kap. 3.11).

Die dem Landeskriminalamt Baden-Württemberg (LKA) bekannt gewordenen Fälle werden nicht gesondert statistisch erfasst. Nach Schätzungen des Dezernats 411 des Landeskriminalamtes Baden-Württemberg liegt die Zahl der Schadensfälle in Ba-Wü bei ca. 20- 30. Hierbei handelt es sich um die zur Anzeige gebrachten Fälle. Da die Geschädigten der Nigeria Connection oft den Schaden verheimlichen, gibt es eine hohe Dunkelziffer. Die Schadenssummen sind sehr unterschiedlich: von 4-stelligen bis zu hohen 6-stelligen Beträgen ist die Rede (E-Mail von Klaus Benzenhöfer, Landeskriminalamt Stuttgart vom 2002-09-20). Einer Anfrage beim Bundeskriminalamt Wiesbaden zufolge gibt es auch auf Bundesebene keine repräsentativen statistischen Angaben über Gesamtzahl der Betrugsoffer, insgesamt versendete Nigeria-Briefe, Anzahl über bisherige Strafanzeigen und Ermittlungsverfahren sowie die gesamte Schadenssumme, die durch die Nigeria Connection entstanden sind. Es erfolgt keine Registrierung des Betrugsdeliktes Nigeria Connection im eigenen polizeilichen Meldedienst. In der polizeilichen Kriminalstatistik PKS fällt dieser zwar in den Bereich der Wirtschafts- und Computerkriminalität, wird aber nicht genau erwähnt (telefonische Mitteilung von Wolfgang Strehmel, Bundeskriminalamt Wiesbaden, Abteilung Öffentlichkeitsarbeit vom 2002-09-30). Aufgrund dieser Aussage werden aus einschlägigen Presseartikeln einige Zahlen zusammengetragen, die durch Schätzungen der Ermittler entstanden sind. 200 Mio. DM Schaden in Deutschland, davon 50 Mio. Mark allein in Berlin (vgl. Hirschbiegel: Zaubерlösung, 2001, S. 20 und Stark: Kriminelle Nigerianer, 2000, S. 12). Auf 3,5 Milliarden Mark schätzt Interpol den volkswirtschaftlichen Schaden allein in Großbritannien. In London sind in einem Jahr 600.000 und weltweit 20 Millionen Nigeria-Briefe mit gefälschten Briefmarken abgefangen worden (vgl. Wolf: Farbe des Geldes, 2000, S. 27 und Kap. 3.5). In Baden-Württemberg sind zwei Fälle mit einem Schaden von je

100000 und 470000 US\$ zur Anzeige gebracht worden (vgl. Troebs: Nigeria-Connection, 1995, Kopie aus Archiv).

3.10 Zielgruppe

Wer erst einmal auf der Liste der Nigeria Connection steht, wird mit Briefen versorgt. Mit dem Adjektiv penetrant lässt sich der Zustand der scheinbar endlosen Briefflut am besten beschreiben: in störender Weise aufdringlich.

Wer steht auf der Liste und welche Voraussetzungen muss man erfüllen, damit man zur Zielperson und zum potentiellen Opfer der Nigeria Connection wird? Das Zahlenmaterial der Betrugsoffer ist nicht repräsentativ genug, um eine vollständige Liste aufzuzeigen. Es ist ein kriminelles Geschäft, kriminell von Seiten der Betrüger und der Betroffenen, weil auch von deutscher Seite oft Schwarzgeld im Spiel ist (vgl. Gea: Kriminelle aus Nigeria, 1996, Kopie aus Archiv). Die Dunkelziffer wird als sehr hoch eingestuft, da viele Opfer auf eine Anzeige verzichten, weil sie sich schämen, hereingelegt worden zu sein (vgl. Poldervaart: Post aus Afrika, 1998, S. 18). Mit Spekulationen versucht das BKA annähernd an die tatsächliche Zahl der angeschriebenen Unternehmen und Einzelpersonen heranzutreten. 30 000 Nigeria-Briefe sollen wöchentlich weltweit verschickt werden (vgl. Zietan: Millionen-Einbahnstraße, 2002, <http://www.spiegel.de/netzwelt/netzkultur/0,1518,186621,00.html>). Das Kriterium mit der höchsten Priorität, das eine Zielperson der Nigeria Connection erfüllen muss, ist die Eigenschaft vermögend zu sein. Die Nigeria Connection hat in den Anfangsjahren vorwiegend auf mittelständische Unternehmen den Fokus gerichtet. Großunternehmen haben oft eine eigene Rechtsabteilung und zählten daher nicht zum engeren Kreis. Neugründungen, die in den Anfangswehen stecken, kommt eine Finanzierungshilfe gelegen. Seit dem erstmaligen Auftreten der Nigeria-Briefe hat sich der Kreis der Zielgruppe ausgedehnt. Selbst Privatpersonen sind nun Angriffsoffer geworden. Die Adressen beschaffen sich die Mitglieder der Nigeria Connection aus öffentlich zugänglichen Quellen wie Telefonbüchern, Handelsregisterauszügen, Branchenbüchern und Messe- und Ausstellungskatalogen (vgl. Winistörfer: Jagd nach Millionen, 1995, S. 21). Dass es sich dabei um reine Willkür bei der Auswahl der Opfer handle, ist nicht bewiesen, jedoch anzunehmen. Äußerst sorgfältig gehen die nigerianischen Abzocker mit dem Adressenmaterial nicht um. Nicht nur Unternehmer werden aufgefordert ins Millionengeschäft einzusteigen, sondern auch Polizeidienststellen, Zollämter, Bundes- und Landesministerien, die Industrie- und Handelskammer Reutlingen, der baden-

württembergische Innenminister Thomas Schäuble (CDU) und selbst der LKA-Präsident in Stuttgart (vgl. Troebbs: Nigeria-Connection, 1995, Kopie aus Archiv). Eine besonders amüsante Fehlleitung des Nigeria-Briefes beschreibt der Journalist Mäder. „Auch lassen sie [die Kriminellen] es mitunter an der zu unterstellenden Sorgfalt fehlen: Unlängst wurde unter der Adresse ‚Kunsthaus Zürich‘ auch ein gewisser Giovanni Segantini brieflich kontaktiert – erwiesenermassen ohne zählbaren Erfolg, verstarb doch der grosse Schweizer Maler bereits anno 1899“ (Mäder: Nigeria-Nepper, 1994, S. 4). Die Bandbreite der angeschriebenen erhofften Opfer ist beachtlich: Ärzte, Politiker, Grafikateliers, Mode-Unternehmen, Mietervereine, Immobilienmakler, Müllfirmen, „kleine Geschäftsleute aus der Provinz erhalten die verlockenden Angebote ebenso wie Weltfirmen in der Größenordnung von Siemens...“ (Gerny, Via Lagos, 1994, S. 6).

Seit ca. 3 Jahren (seit ca. 1999) nimmt die Nigeria Connection auch über E-Mail Kontakt zu den potentiellen Opfern auf. Ob sie sich bei der Beschaffung auf frei zugängliche E-Mail-Verzeichnisse, auf Verteilerlisten oder auf andere Quellen stützt, ist fraglich. Eine Ausweitung und Veränderung der Zielgruppe kann durch die Möglichkeit des E-Mail-Versandes festgestellt werden. Abgesehen von der einmaligen technischen Basisausstattung (PC, Modem, etc.) muss die Nigeria Connection fast kein Geld für die Angebotsschreiben mittels E-Mail investieren. Die Nigeria-Briefe unterliegen bei der Auswahl der Zielpersonen nicht mehr einer sorgfältigen Prüfung, was bei konventionellen Briefen und Telex noch Geltung hatte (vgl. Kap. 3.8.1). Durch die mangelnde Umsicht bei der Auswahl muss wohl damit gerechnet werden, dass private Personen ohne geschäftliche Verbindung E-Mails aus Nigeria erhalten.

3.10.1 Untersuchung der Zielgruppe

3.10.1.1 Professoren als Zielgruppe?!

Im Falle der Professorin²² wurden folgende Überlegungen angestellt: die Nigeria-Briefe werden an ihre Hochschuladresse geschickt, nicht an ihre private E-Mail-Adresse. An der Fachhochschule selbst scheint bislang noch kein anderer Mitarbeiter von Briefen der Nigeria Connection betroffen zu sein. Von den Studenten ist auch noch niemand angeschrieben worden (mündliche Mitteilung von Margarete Payer vom 2002-07-28 nach Befragung von Studierenden). Eine Hochschuleinrichtung und deren Mitglieder

²² siehe nähere Schilderung in Kap. 3.1

gehören nicht zur favorisierten Zielgruppe der nigerianischen Wirtschaftskriminellen, da keine allzu großen Vermögenswerte zu erwarten sind. Die E-Mail-Adresse steht zwar im Professorenverzeichnis auf der Website der Hochschule, ein Kontakt zu anderen Professoren wäre jedoch die logische Folge gewesen. Wenn die E-Mail-Adresse unwissentlich in einem anderen Verzeichnis aufgeführt ist, könnte das zumindest eine brauchbare Erklärung sein. Wie jedoch davon ausgegangen werden kann, dass sich hinter dieser E-Mail-Adresse (payer@hdm-stuttgart.de) ein potentielles Neuopfer verbergen könnte, ist nicht nachvollziehbar. Tiefere Recherchen bleiben aus, sonst würden die Nigeria-Briefe wohl kaum mit „Dear Sir“ beginnen. Vermutungen, der E-Mail-Kontakt zu einem selbst von Nigeria-Briefen betroffenen Reisebüro könnten die Lösung sein, sind spekulativ. Sie vermutet, dass der Zugriff (durchschnittlich 3000 Zugriffe täglich) auf die privaten Webseiten, die in den üblichen Suchmaschinen nachgewiesen werden, die Kriminelle glauben lassen, dass ein zahlungsfähiger Geldgeber hinter den Webseiten steht. Auf der Webseite ist immer die offizielle E-Mail-Adresse angegeben. Die Professorin geht heute (September 02) davon aus, dass die Kriminellen eher Roboter einsetzen, die stark angefragte Internetseiten herausfiltern und automatisch die E-Mail-Adressen liefern. Allerdings ist das schwer nachweisbar.

Einer der zu untersuchenden Nigeria-Briefe bestätigt jene Vermutung, ein handfester Beweis für die grundsätzliche Vorgehensweise ist das nicht.

„I got your contact from the google search engines“ (E-Mail von der Nigeria Connection vom 2002-07-22).

3.10.1.2 Analyse der Zielgruppe durch telefonische Stichproben

Um die Angaben aus den Pressemitteilungen und meinen einschlägigen Interviews mit Kriminaloberkommissar Wolfram Künkele, Polizeidirektion Reutlingen, Kriminalinspektion 3 vom 2002-07-31, Klaus Benzenhöfer, Landeskriminalamt Baden-Württemberg in Stuttgart, Dezernat 411 vom 2002-09-20 und Wolfgang Strehmel, Landeskriminalamt in Wiesbaden, Abteilung Öffentlichkeitsarbeit vom 2002-09-30 zu verfestigen, wurde ein Stichprobenverfahren angewendet. Die Stadt Reutlingen gehört mit 109398 Einwohnern (Stand September 02) zu den größeren Städten im süddeutschen Raum. Rund 7000 gewerbliche Meldungen existieren in genanntem Zeitraum im Stadtkreis Reutlingen. Nach telefonischer Auskunft des Statistischen Landesamtes Stuttgart erfolgt keine Einteilung in die Unternehmensgrößen Großunternehmung, mittelständische Unternehmung und Einzelunternehmung. Das Stichprobenverfahren erfolgte tele-

fonisch. Die Auskunft erteilte entweder die Personalabteilung oder der Inhaber des Unternehmens. Keine der ausgewählten Firmen mußte besondere Kriterien erfüllen. Die Zuordnung in die erklärte Kategorie war einziges Kriterium. Jeweils drei Firmen der jeweiligen Kategorien sind nach der Existenz der Nigeria Connection und deren Kontaktaufnahme zur Firma befragt worden. Das Ergebnis: nur eine Firma von insgesamt neun völlig willkürlich ausgewählten Firmen wies die Frage nach der Kontaktaufnahme der Nigeria Connection ab. Aus Zeitungsartikeln und einer Warnmeldung der im Landkreis Reutlingen ansässigen IHK war der Geschäftsinhaberin diese Betrugsform jedoch bereits bekannt. Bei der von der Nigeria Connection noch verschonten Firma handelt es sich um ein Blumengeschäft, Einzelunternehmung. Ein Stichprobenverfahren spiegelt nicht zwangsläufig den allgemeinen Zustand der Gesamtmasse wider. Der Bekanntheitsgrad der Nigeria Connection kann jedoch durch diese Testanrufe im Landkreis Reutlingen als hoch eingestuft werden.

3.11 Psychologie

Die Angaben des BKA über die Anzahl der Betrugsoffer wirft die Frage auf, weshalb man auf die Forderungen der Nigeria Connection überhaupt eingehen kann. Die Angebotsschreiben werden zwar taktisch formuliert, dem wachen Verstand des Angesprochenen sollte sich prinzipiell während des Lesens der Briefe der Verdacht des Betrugsversuchs aufzwingen. Vorkenntnisse und politische Hintergründe zu Nigeria müssen nicht vorhanden sein, um Zweifel an dem angebotenen Millionentransfer aufzubringen. Die Tatsache, dass eine wildfremde Person aus einem außereuropäischen Land, die zuvor weder eine geschäftliche noch eine private Beziehung zu dem Angesprochenen hatte, sich an ein Unternehmen wendet, das wegen seiner Seriosität und Kompetenz auserwählt wurde, einen Geldbetrag in Millionenhöhe aufgrund größtem Vertrauen entgegenzunehmen, sollte Grund genug sein, dieses Angebot ernsthaft zu hinterfragen. Der gesunde Menschenverstand wird durch Habgier, Naivität, Risikobereitschaft und die Aussicht auf schnelles Geld ersetzt. Dies sind die auslösenden Faktoren, die die Angesprochenen dazu bewegt, sich auf ein illegales Geschäft einzulassen (mündliche Mitteilung von Kriminaloberkommissar Wolfram Künkele vom 2002-07-31). Die Zahl der tatsächlichen Betrugsoffer ist nicht erfassbar. Den Geschädigten ist ihre Gutgläubigkeit peinlich und geben nur ungern zu, auf das anrühige Angebot reagiert zu haben (vgl. Wolf: Farbe des Geldes, 2000, S. 27).

Die Betrachtung der Zielpersonen der Nigeria Connection zeigt, dass es sich bei den meisten Angesprochenen um Unternehmer handelt (vgl. Kap. 3.10). Ein Unternehmer muss sich u. a. mit Führungsaufgaben und dem richtigen Umgang mit Mitarbeitern auseinandersetzen. Eine Person, der Führungsqualitäten und Managementfunktionen anvertraut werden, darf angesichts des zu verdienenden Geldes nicht unüberlegt handeln und u. U. die Existenz des Unternehmens gefährden. Nach Kontaktaufnahme zu den Betrügern stehen die angehenden Opfer unter Stress und handeln unüberlegt. „Es geht um viel Geld und sie [die Opfer] tun etwas illegales“ (Wolf: Farbe des Geldes, 2000, S. 27). Die Psychologie der Nigeria Connection bewährt sich. Sie setzt auf unterschiedliche Taktiken: die geschäftliche, mitleiderregende oder fromme Masche weckt bei wenigen, aber ausreichend vielen Empfängern der Nigeria-Briefe Interesse.

3.12 Verhaltensvorschläge, Kontaktadressen und Maßnahmen

Auf der Website des Bundeskriminalamtes wird in drei Worten festgehalten, wie man mit den bedenklichen Nigeria-Briefen umzugehen hat: „Nie antworten! Wegwerfen!“ (Polizei Ba-Wü: Warnmeldungen, 2002, http://www.polizei-bw.de/fahndung/warmmeldung/warmmeldungen_nigeria.htm). Man solle nicht einmal im Sinne einer Absage antworten. Wird dies auf dem herkömmlichen Briefweg getan, kommen die Kriminellen in den Besitz von Originalunterschriften, Geschäftsbögen, Bankverbindungen und Telefonnummern. Weitere betrügerische Handlungen wie z.B. Vollmachten, Visagesuche und Banktransaktionen sind realisierbar (vgl. Kap. 3.6). Der Ratschlag, auf dubiose Briefe, Faxe und E-Mails nicht zu reagieren und diese zu vernichten und löschen, wird von den meisten Empfängern auch ohne vorherige Anweisung automatisch ausgeführt. Nach Zietan werden 99% dieser Köder-Mails an die Angesprochenen auch dorthin befördert, wo sie hingehören – in den digitalen Mülleimer. Das verbleibende Prozent geht auf das Betrugs-Angebot ein (vgl. Zietan: Millionen-Einbahnstraße, 2002, <http://www.spiegel.de/netzwelt/netzkultur/0,1518,186621,00.html>). Die bereits erwähnte Website der Polizei Baden-Württemberg sowie die Internet-Präsenzen des Bundeskriminalamtes raten dann eine Strafanzeige zu erstatten, wenn „sich [Empfänger] betrügerisch geschädigt fühlen“ (Polizei Ba-Wü: Warnmeldungen, 2002, http://www.polizei-bw.de/fahndung/warmmeldung/warmmeldungen_nigeria.htm). Liegt noch kein finanzieller Schaden vor, so ist die Weiterleitung der Nigeria-Briefe an die örtliche Polizeidienststelle dennoch erwünscht. Jene werden zu Stapeln angehäuft und an die entsprechende Landesdirektion weitergeleitet.

Ein Verfahren, d. h. eine Strafanzeige gegen die Nigeria Connection, kann nur bei persönlichem und finanziellem Verlust eingeleitet werden. Da es sich bei den Kontaktaufnahmen um eine straflose Vorbereitungshandlung handelt (vgl. Kap. 3.9), wird i. d. R. der Brief als weiteres Beispiel zur Kenntnis genommen. Jeder Hinweis trägt dazu bei, Strukturen und Zusammenhänge aufzuhellen und die Ergreifung der Täter voranzutreiben.

Das Auswärtige Amt in Berlin ist ein weiterer Ansprechpartner auf dem öffentlichen Sektor. Auf seiner Website präsentiert es Hinweise, Erläuterungen und Verhaltenstipps zum Vorauszahlungsbetrug Nigeria Connection. Unter dem Themenpunkt „was man tun sollte“ erhält der Internet-Besucher ebenfalls den Hinweis, zur nächsten lokalen Polizeidienststelle zu gehen. Des weiteren soll man „den Vorfall bei der nigerianischen Auslandsvertretung in ..[seinem] Lande“ melden und den digitalen oder konventionellen Brief an aufgelistete Adressen in Nigeria schicken. Der Schlusssatz „eine Verfolgung zivilrechtlicher Ansprüche ist so gut wie ausgeschlossen“ spiegelt den bereits im vorigen Abschnitt erwähnten Sachverhalt wider, dass die Rechtslage äußerst kompliziert ist (Auswärtiges Amt: Hinweise Nigeria-Connection, 2002, http://www.auswaertiges-amt.de/www/de/laenderinfos/419_html)²³.

Neben den durch die Nigeria Connection bekannten Ministerien und Banken existieren auch seriöse nigerianische Geschäftszweige. Diese haben durch den schlechten Ruf, den Nigeria durch die Betrügerbriefe erlangt hat, große Einbußen erlitten (vgl. Henauer: Betrügerbanden, 2002, <http://www.internet.bap.admin.ch/d/aktuell/warnung/n-betrueger.htm>). Um die „weißen“ Schafe der nigerianischen Geschäftswelt von den Betrügern differenzieren zu können, stellt die Schweizer Zentrale für Handelsförderung (OSEC) schwarze Listen auf. Vor Geschäftsabschluss mit einem nigerianischen Handelspartner können diese eingesehen werden (vgl. Maise: Nigeria-Millionen, 1996, S. 10).

²³ Im Anhang B.1 befinden sich Kontaktadressen und Links zu Verhaltensvorschlägen.

Abzocker im Internet wenden unterschiedliche Taktiken an, um von finanziellen Gewinnen profitieren zu können. Die 0190-Abzocker, die im nächsten Themenblock vorgestellt werden, bedienen sich des gleichen Telekommunikationsinstrumentes, sie verwenden dies jedoch in seiner allgemeinen Rundumwirkung. 0190-Dialer sind raffinierter und nehmen keinen offensichtlichen Kontakt zu den Zielpersonen auf, sondern schleichen sich ohne Vorankündigung auf die Festplatte des Computers. Im Unterschied zu der Nigeria Connection gehören zur Zielgruppe der 0190-Dialer nicht die Unternehmen, sondern jeder Nutzer des Mediums Internet, wobei überwiegend Jugendliche und männliche Personen erreicht werden (mündliche Mitteilung von Kriminaloberkommissar Wolfram Künkele vom 2002-10-22). Durch Gutgläubigkeit und Naivität der Angesprochenen gewinnt die Nigeria Connection ihre Opfer, die psychologischen Köder der 0190-Abzocker sind Neugier und Unachtsamkeit. Da es keine gesonderten statistischen Angaben zu erfassten Betrugsopfern und Schadenssumme der Nigeria Connection gibt, wird auf eine Gegenüberstellung dieser beiden Abzocker in Hinblick auf Anzahl der Betrugsfälle, Anzahl der Opfer, bisherige Geldverluste, etc. verzichtet. In beiden Themenblöcken wird in den Kapiteln der Rechtsverfahren auf Zahlenmaterial hingewiesen, das mit Hilfe des Bundeskriminalamtes Wiesbaden und des Landeskriminalamtes Baden-Württemberg sowie einschlägigen Pressemeldungen entnommen werden konnte.

4 0190-Dialer

„Beutelschneider, die Schindluder mit kostspieligen 0190-Nummern treiben“ (Jutzi: Nepper, Schlepper, Surferfänger, 2001, S. 104).

4.1 Wahl des Themas

Eine durch Raffinesse und Skrupellosigkeit gekennzeichnete Art von Abzocke ist das Eindringen einer Software auf den Rechner, die einen unmittelbaren finanziellen Schaden hinterlässt und von der Ahnungslosigkeit des Internetnutzers profitiert. Die 0190-Dialer zählen noch nicht lange zu den Problemkindern der gesamten Computerkriminalität. Betroffen können sämtliche Internetnutzer werden. Diese Form der organisierten Internet-Kriminalität wird aus Gründen der Aktualität untersucht. Während der Abfassungszeit der Diplomarbeit wurde der Änderung der Telekommunikations-Kundenschutzverordnung gegen den Missbrauch der Mehrwertdiensterrufnummern (0190er Nummern) vom Bundesrat zugestimmt. Dieser Themenblock soll kein Ratgeber für Geschädigte oder interessierte Internetnutzer darstellen, sondern eine weitere Form von Cyber-Kriminalität aufzeigen, deren primäres Ziel die Abzocke meist unschuldiger User ist. Der Themenblock versteht sich vielmehr als Warnhinweis, dass das streunende Surfen mit fehlender Aufmerksamkeit sehr teuer werden kann. Hilfreiche Internetseiten für Interessenten und Kontaktadressen für Geschädigte werden im Anhang B.2 aufgelistet.

Cyber-Kriminalität ist so schnelllebig wie das Internet selbst. Kriminelle suchen sich immer wieder neue Nischen für betrügerische Aktivitäten. Die 0190-Abzocker greifen aus dem Hinterhalt an, der Kontakt zu ihnen wird offensiv durch Internetnutzer über harmlos wirkende Websites hergestellt. Ein einziger Klick auf den Link einer Website oder ein bestätigendes OK eines sich öffnenden Hinweisfensters reichen aus, den Download des Dialer-Programms zu starten. Diese Art von Kriminalität zeichnet sich durch einen Einschleichungsprozess aus, dessen Auswirkungen die ahnungslosen Betroffenen über die Telefonrechnung unvorbereitet trifft. Die Betrüger (be)nutzen die Telekom als Netzbetreiber und Rechnungssteller, um den finanziellen Gewinn zu erhalten.

Mit Stand Mai 02 wurde der Dialer-Betrug als erfolgreichste Abzock-Methode im Internet deklariert (vgl. Spiegel: Gesetz ist durch, 2002, <http://www.spiegel.de/netzwelt/politik/0,1518,207650,00.html>).

4.2 0190-Dialer, getarnte Eindringlinge

Das Internet stellt eine ideale Plattform für Trickbetrüger dar. Eine besonders listige Methode machen sich die Gauner und Ganoven zunutze, die durch das unbemerkte Aufdrängen eines 0190-Dialer bei Internetnutzern und Besuchern einschlägiger Websites finanziellen Gewinn schöpfen und den ahnungslosen User schröpfen können. Dialer (englisch *to dial* = wählen) lässt sich mit Wählprogramme übersetzen. Verschiedene Bezeichnungen existieren für diese Art von Abzocke, u. a. 0190-Abzocke, Dialware, 0190er-Trojaner. Die populärste Bezeichnung ist 0190-Dialer, und wird daher in dieser Diplomarbeit verwendet.

4.2.1 Technische Grundlage der Dialer: Trojanische Pferde

0190-Dialer sind eine spezielle Art von Trojaner²⁴, die eine unmittelbare finanzielle Schädigung mit sich bringen:

„Ein Trojaner ist ein Programm, das vorgibt, eine wünschenswerte oder notwendige Funktion auszuführen und das möglicherweise auch tut, aber außerdem eine oder mehrere Funktionen ausführt, die die Person, die das Programm ausführt, weder erwartet noch wünscht“ (hacker's guide, 2001, S. 433). Um die Existenz und die Platzierung eines Trojaners zu verbergen, geben sie sich meist als vermeintlich nützliche Programme aus und verstecken sich hinter Spielen, Scherzprogrammen, Bildschirmschonern, u. a. Der Trojaner spioniert versteckt im Hintergrund. Trojaner sind demnach Programme, die heimlich oder unter Vorspielung unechter Tatsachen in einen Computer geschleust werden und dort selbständig oder mittels Fernsteuerung Schäden anrichten bzw. Daten ausspionieren können. Ein Trojaner bewirkt eine Veränderung des ursprünglichen Programms und ist damit ein „unautorisierter Code innerhalb eines legitimen Programms“ (Vosseberg: hackerz book, 2002, S. 120). Die einfachste Möglichkeit, ein trojanisches Pferd auf einem Fremdrechner zu installieren, ist das Internet oder ein Netzwerk.

²⁴ Trojanische Pferde, kurz als Trojaner bezeichnet

4.2.2 Vorgehensweise der 0190-Dialer

Im Internet stehen verschiedenste kostenpflichtige Dienstleistungen zur Verfügung, die über Dialer-Programme aufgerufen und abgerechnet werden können. Die Aktivierung eines Dialer-Programmes bewirkt die Trennung der aktuellen Browserverbindung und den Aufbau einer wesentlich teureren Verbindung über den 0190-Service. Dieser Vorgang kann sich unbemerkt abspielen, so dass der Internetnutzer den Eindruck hat, die ursprüngliche Internetverbindung wurde nicht unterbrochen und die gewünschten Informationen erhielt er ohne weitere Kosten. Das unbemerkte Herunterladen ist das Kapital der Dialer-Anbieter. Seriöse 0190-Anbieter weisen auf die kostenpflichtige Verbindung hin, die mit der Bestätigung des Downloads beginnt. Zusätzlich wird i. d. R. die Wirkungsweise genau erklärt. Verschleierte oder keine Kostenhinweise zeichnen unseriöse Anbieter aus. Nach Verlassen des Internetangebots erfolgt weder eine Trennung der Verbindung noch deaktivieren sich die Dialer-Programme automatisch, sondern vermitteln bei jedem erneuten Einwählen ins Internet die hochpreisige Verbindung der 0190er-Nummer. Einige Dialer-Programme tragen sich als Standardverbindung in die Datei des DFÜ-Verzeichnisses ein (vgl. RegTP: Informationen 0190-Dialer, 2002, <http://www.regtp.de/service/02501/01/index.html>). Das kriminelle Verhalten der legitimen 0190-Dialer fängt an dem Punkt an, wenn kein ausdrücklicher Wunsch oder keine Dienstleistung, die über eine Mehrwertnummer abgerechnet werden soll, verlangt und angefordert wird.

Die 0190-Nummern sind als Möglichkeit einer unproblematischen und anonymen Zahlungsmethode eingeführt worden. Das Abrechnungssystem hat für alle Dienste, die über die Telefonleitung erbracht werden, Geltung und betrifft daher den Telefon-, Fax- und Internetanschluss. Dienstleistungen können ohne Bekanntgabe der Bankverbindung oder der Kreditkartennummer über die Telefonrechnung beglichen werden. Da der Anbieter die Kosten für die Verbindung selbst bestimmen kann und keine Preisobergrenze existiert, sind diverse Angebote dementsprechend teuer. Das Abrechnungssystem erfolgt entweder als Minutenpreis oder als Einmalpreis pro Einwahl (vgl. Mack: Fax spuckt alte Information, 2002, S. 17). Es existieren Dialer, die die Internetverbindung immer wieder neu aufbauen, weil ihr Anbieter pro Einwahl kassiert²⁵.

²⁵ Es ist ein Fall bekannt, bei dem der Anbieter mit diesem Abrechnungssystem 900 Euro in Rechnung stellte.

Eine andere Möglichkeit, den Kunden abzuzocken, ist die Kennzeichnung der angebotenen Leistung mit einem scheinbar günstigen Minutenpreis.

Im Kleingedruckten wird dann näher erläutert, dass der Abrechnungstakt beispielsweise 90 Minuten beträgt – d.h. auch wenn man das Angebot nur wenige Minuten nutzt, wird mindestens 1 Abrechnungstakt berechnet.

Was bisher vor allem von Betreibern der Erotik- und Sexwebsites angeboten wurde, wird nun durch hinterhältige Täuschung und Irreführung der Internetnutzer auch von scheinbar harmlosen Website-Anbietern praktiziert. Die Abzocker treten aus der Schmutzdecke der Sex- und Erotikseiten hervor. Kostenlose Downloads von Bildern und Filmen werden auf den Seiten angepriesen. Um sich die Bilder anzusehen, bedarf es einer speziellen Zusatzsoftware. Hinter dieser verbirgt sich das Dialer-Programm. Völlig automatisch ohne Bestätigung installieren sich Dialer-Programme in den seltensten Fällen, das unachtsame Wegklicken eines Fensters oder Klicken auf eine Schaltfläche startet den Download. Eine erfolgreiche Masche der 0190-Abzocker ist die Vortäuschung eines Nutzens. „Kontakte (Partnersuche, Modelcasting), Links auf ‚geheime‘ Seiten, mehr Funktionen für bekannte Programme wie den Internet Explorer oder ‚Highspeed‘-Internet. Alles Humbug“ (Test: Nepp mit 0190, 2002, S. 32). Eine angeblich unablässige, aber kostenfreie Programmerweiterung wird als Vorwand angemahnt, um den Download zu starten. Das Programm kostet in der Tat nichts, über die Telefonrechnung erhält der Anbieter sein Geld. Die heimtückischste Falle ist die Realisierung der Schaltfläche durch das Fenster selbst. Ein Schließen-Button existiert nicht und das Anklicken in das Fenster startet den Download (vgl. Test: Nepp mit 0190, 2002, S. 32). Da diese Programme nicht umfangreich sind, dauert der Download-Vorgang nicht lange (max. 2-3 Sekunden) und kann daher unbemerkt ablaufen.

DSL-Internetzugänge sind prinzipiell vor Dialern sicher, wenn beim PC die zuvor genutzte Analog- oder ISDN-Verbindung nicht parallel weiterbetrieben wird. Bei DSL findet keine Einwahl über die Telefonleitung statt. Durch einen manuellen Handgriff wird Abtrennung des Modem- oder ISDN-Kabels oder durch die komplette Deinstallation der entsprechenden Hard- und Software erzielt (Test: Nepp mit 0190, 2002, S. 32). Die meisten Internetnutzer verwenden Windows-PCs. Dadurch entsteht eine lohnende Angriffsfläche für Dialer-Programme, die in Windows-Systemen ihre Wirkung haben.

Durch die Möglichkeit der Bereitstellung der 0190-Dienste über die Telekommunikationsmittel Telefon, Fax und Handy²⁶ erzielen die Abzocker einen hohen Abschöpfungsgrad von fremden Geldern und gehen somit nicht nur über das Internet auf Opferfang. Zwar wird bei Telefon und Faxgerät kein Dialer-Programm installiert, die erfinderischen Ganoven der Telekommunikationswelt treiben die Telefonrechnungen der Kunden jedoch ebenfalls in unerwartete Höhe. Der finanzielle Schaden durch die Tricks rechnet sich, sonst würde es keine ausdrückliche Warnmeldungen von Seiten der Polizei geben (vgl. Polizei Ba-Wü: Trickbetrüger, 2002, http://www.polizei-bw.de/fahndung/warnmeldung/warnmeldungen_0190.htm). Die 0190-Abzocker sind erfinderisch und werden auch künftig jede sich ergebene Möglichkeit nutzen. Oft ist es Neugier, die die Angeschriebenen oder Angerufenen dazu veranlasst, den Aufforderungen nachzukommen (vgl. Mack: Fax spuckt alte Information, 2002, S. 17).

4.3 Fallbeispiel: Opfer der 0190-Abzocke

Mit raffinierten Verschleierungstricks locken die Abzocker den User mitunter auf zunächst harmlos wirkende Websites und installieren dadurch den Dialer. Durch E-Mails, die als Rundschreiben fungieren, wird auf den Link aufmerksam gemacht oder der Dialer befindet sich im Attachment der E-Mail. Zwar erreicht das Dialerproblem einen hohen Streuungsgrad, eine richtige Gefährdung stellt es jedoch für Jugendliche und Chatroom-Surfer dar (vgl. Kap. 4.5). Im folgenden werden zwei Fälle beschrieben, die einerseits stellvertretend für die primäre Zielgruppe und andererseits für die klassische Vorgehensweise der 0190-Abzocker sein sollen.

Der Journalist Philipp Scheffbuch berichtet über einen jungen Mann, der sich die Dialer-Software unwissentlich installierte. Auf der Suche nach einem Online-Flirt surft der 21-jährige in einem Chatroom, bis er fündig wird. Ein nettes Mädchen hat es ihm angetan. Um sie in ihrer ganzen Schönheit zu bewundern, solle er auf ihrer persönlichen Homepage vorbeischauen. Der junge Mann hatte Interesse und klickte auf den im Chat ange-

²⁶ SMS-Nachrichten in Form von „Du siehst toll aus, bist sexy und charmant. Ruf mich an unter 0190 - ...“ und ähnliche Liebesbotschaften werden mit dem Hinweis um Rückruf im Massenversand verschickt. Wird der Aufforderung Folge geleistet, wird durch eine endlos dauernde Bandansage der vermeintlich Auserwählte am laufenden Gebührenzähler gehalten. Eine andere Variante der Abzocker ist die Versendung von unbestellter Ware, deren Reklamation nur über eine 0190-Nummer möglich ist. Oder Reisebuchungsbestätigungen, die niemals in Auftrag gegeben worden sind, deren Stornierung auch nur über eine 0190-Nummer durchführbar ist. Auf privaten Anrufbeantwortern wird der Text „Bitte rufen Sie mich zurück“ und eine 0190-Nummer hinterlassen (vgl. Polizei Ba-Wü: Trickbetrüger, 2002, http://www.polizei-bw.de/fahndung/warnmeldung/warnmeldungen_0190.htm).

gebenen Link. Die Website entpuppte sich als Flop, daher verließ er die Site und widmete sich wieder seiner Suche im Chatroom. Bei der nächsten Telefonrechnung wollte ein ihm unbekannter Anbieter einer 0190er Rufnummer satte 1700 Euro in Rechnung stellen. Statt des Dates hatte sich der 21-jährige unwissentlich einen Dialer eingefangen. Den Rechnungsbetrag hat er bei der Telekom reklamiert. Da die Telekom zwar die Rechnungen erstellt, jedoch die 0190er-Nummern nicht betreibt, wurde er aufgefordert, die DFÜ-Verbindungen auf seinem Rechner auf die 0190-Dialer zu überprüfen. Da er nach seinem Besuch auf der Köder-Website einen Freund gebeten hatte, ein neues Betriebssystem zu installieren, wurde der Webdialer inklusive Kennung von der Festplatte gelöscht. Der Journalist erwähnt nicht, ob die 1700 Euro Telefonrechnung bezahlt werden musste.

In einem anderen Fall sollte eine Mutter 9000 Euro Dialer-Gebühren aufbringen, da ihr Sohn beim Surfen einen Dialer heruntergeladen hatte, der auch bei allen anderen Internetverbindungen aktiviert blieb. Der jugendliche Sohn konnte sich zwar an keinen Hinweis erinnern, der ihm die Bestätigung des Dialer-Downloads mitteilte, vor Gericht wurde die Anzeige der Mutter gegen den 0190-Abzocker jedoch wegen keiner offensichtlichen Täuschung und keinem sittenwidrigen Verhalten des Anbieters abgelehnt (vgl. Scheffbuch: Teurer Flirt im Netz, 2002, S. 37).

4.4 Rechtliche Strafverfolgung

Straftaten im Internet nehmen zu. Durch die Problematik der Lokalisierung der Betrüger und die Schnelllebigkeit des Internets (Websites haben oft eine geringe Lebenserwartung) ist ein Rechtsverfahren häufig problematisch und zeitaufwendig. Hinzu kommt oftmals ein Daten- und Informationsaustausch über die deutschen Grenzen hinweg. Die Belangung der kriminellen Abzocker, deren Sitz sich im Ausland befindet, obliegt dem in dem jeweiligen Land gültigen Recht. Die problematischste Voraussetzung für ein Ermittlungsverfahren gestaltet sich wie folgend: die 0190-Abzocker tarnen sich hinter Briefkastenfirmen, die Inhaber sind nicht auffindbar oder leben im Ausland. Dem justitiellen Arm sind Grenzen gesetzt, wenn der Betrug nicht in beiden Ländern als Betrug angesehen wird.

Bei nachvollziehbarer kriminellen Handlung kann gegen den Anbieter der 0190er-Nummer und den Initiator der Dialer-Installierung Anzeige erstatten werden. Ein Verstoß gegen die legitime Nutzung der Mehrfachnummern kann aufgrund der protokollier-

ten Eintragungen des DFÜ-Verzeichnisses nachvollzogen werden. In vielen Fällen werden nach Erhalt der überhöhten Telefonrechnung wichtige Daten auf dem PC in einer Art Panikreaktion gelöscht (mündliche Mitteilung von Kriminaloberkommissar Wolfram Künkele vom 2002-10-23). Durch die auf diese Weise verlorengegangenen Hinweise auf den kriminellen Anbieter müssen andere aufschlussreiche Ansatzpunkte für die Kriminalpolizeibeamten geliefert werden. Ein Anwählen der Website, durch die sich der Dialer installiert hat, ist grundsätzlich hilfreich. Die Betroffenen erinnern sich im Regelfall jedoch nicht mehr an die genaue URL, oder die Website ist bereits nicht mehr verfügbar.

Die raffinierte Vorgehensweise der 0190-Abzocker wird nicht nur durch das heimliche Einschleichen auf den Rechner der Internetnutzer, sondern auch durch die anschließende schwierige persönliche Auffindbarkeit aufgezeigt. Die Anonymität im Internet hat für Betrüger dieser Art Vorteile. Eine rechtliche Belangung ist aufgrund ungünstiger Voraussetzungen wegen des Verhaltens der Internetnutzer (Löschung relevanter Daten, Nicht-Erinnern an die URL) prekär und nicht befriedigend realisierbar.

Aus Gründen der zunehmenden Unzufriedenheit und des unzureichenden Schutzes der Bevölkerung vor 0190-Betrug hat die Bundesregierung am 2002-07-31 der Gesetzesänderung der Telekommunikations-Kundenschutzverordnung zugestimmt. Die rechtswidrige Nutzung der Mehrwertdiensterrufnummern soll unterbunden werden. Dem Wunsch, leichter an die Anbieter herantreten zu können, ist man durch die Gesetzesänderung zwar näher gekommen, Zufriedenheit von Seiten der Freiwilligen Selbstkontrolle Telefonmehrwertdienste (FST) e. V., der Polizei und Verbraucherschützer ist nicht erkennbar (Computerwoche: Schutz vor 0190-Abzocke, 2002, S. 8). Durch die Änderung der Telekommunikations-Kundenschutzverordnung lassen sich Dienstleister und Betrüger besser voneinander trennen. Auf den Telefonrechnungen müssen die angewählten 0190-Nummern sowie Name und Anschrift des für die Rechnungsstellung Verantwortlichen angegeben werden. Kunden wird nun die Möglichkeit gegeben, sich bei einer Beschwerde direkt an den Rechnungssteller zu wenden. Netzbetreiber müssen diese bei nachgewiesenem Missbrauch der vergebenen Mehrwertnummern sperren. Es soll künftig verhindert werden, dass die Telekommunikationsfirmen – für gewöhnlich Telekom – trotz Hinweise auf abzockerische Handlungen einfach weiter mit abkassieren (vgl. Spiegel: Gesetz ist durch, 2002, <http://www.spiegel.de/netzwelt/politik/>

0,1518,207650,00.html). Ob sich das Gesetz durch langfristigen Erfolg bei der Eindämmung der 0190-Abzocke stabilisieren wird, kann zum augenblicklichen Zeitpunkt nicht gesagt werden.

Aus der polizeilichen Kriminalstatistik (PKS) des Berichtsjahres 2001 geht ein starker Anstieg im Bereich der Internetkriminalität hervor. Ein wesentlicher Teil wird dabei dem Internetzugangsmissbrauch (Accountmissbrauch) durch Umleitung des persönlichen Provider-Zugangs auf einen 0190er-Zugang mit dann erheblich höheren Verbindungskosten zugeschrieben. Die folgende Tabelle zeigt die erfassten Fälle der 0190-Abzocke und zum Vergleich zwei weitere Betrugsform der Computerkriminalität²⁷, die jedoch nicht extra behandelt werden, sondern nur zur Veranschaulichung dienen.

Tabelle 11: Fallentwicklung Computerkriminalität am Beispiel Internetzugangsmissbrauch

Straftat	erfasste Fälle		Veränderung	
	2001	2000	absolut	in %
Computerkriminalität Gesamt	79 286	56 699	+22 587	39,8
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	8 039	2 198	+5 841	265,7
Ausspähen von Daten	1 463	538	+925	171,9
Betrug mittels rechtswidrig erlangter Karten für Geldausgabe- bzw. Kassenautomaten	48 610	44 284	+4 326	9,8
Softwarepiraterie (private Anwendung z.B. Computerspiele)	1 672	1 361	+311	22,9

[Quelle: BKA: Polizeiliche Kriminalstatistik, 2001, <http://www.bka.de/pks/pks2001/index2.html>]

4.5 Zielgruppe der 0190-Dialer

Betrügerische Aktionen weisen sich, wie andere strategische Methoden auch, oft durch die bewusste Auswahl der zu fokussierenden Zielgruppe aus. Die zielgenaue Lenkung der kriminellen Machenschaften ist durch das Medium Internet nicht unproblematisch, da sich die Nutzerschaft auf viele Altersklassen und Berufsgruppen verteilt. Gewiefte Strategen versuchen aus den Internetnutzern möglichst genaue Nutzerprofile zu erstellen, um diese mit Werbung und Angeboten einzudecken.

²⁷ Die in der PKS verwendete Bezeichnung für Betrugsdelikte im Internet ist Computerkriminalität.

Interessen und Gewohnheiten von Usern sind Ansatzpunkte von Abzockern (vgl. Gieseke: Anti-Hacker-Report, 2002, S. 502).

Im Gegensatz zu der Methodik der Nigeria Connection, deren Zielgruppe primär eine vermögende Berufsschicht ist, nutzen die 0190-Abzocker die Gunst der Popularität des Internets. Die zunehmende Verbreitung des Mediums Internet machen sich diese Internet-Kriminellen zu eigen. Grundsätzlich ist jeder, der über einen Internetanschluss verfügt, potentiell Opfer dieser Art von Abzocke. Die eigentlichen Zielpersonen sind User, die sich noch nicht routiniert im Netz bewegen und fahrlässig mit Sicherheitseinstellungen und –hinweisen umgehen. Vordergründig ist die Neugierde und die Entdeckung der Informationsangebote. Neueinsteiger und Jugendliche können zu der Zielgruppe der Dialer gezählt werden. „Aus meiner beruflichen Erfahrung kann ich sagen, dass das typische Opfer von Dialer-Programmen primär der unerfahrene User ist. In einem Fall war es ein Arzt, der als Neu-User aus typischer Neugier einschlägige Sexseiten absurfte“ (mündliche Mitteilung von Kriminaloberkommissar Wolfram Künkele vom 2002-07-31). Statistische Erhebungen über Internetentwicklung zeigen den hohen Anteil von Surfern der Altersgruppe der 14-29-jährigen im Vergleich zu der Gesamtzahl der Nutzer auf (vgl. Kap. 2.2).

Durch wirres Erscheinen von nacheinander geschalteten Pop-up Fenstern verlieren ungeübte Nutzer schnell den Überblick und klicken in ebenso wirrer Weise auf Fenster, deren Meldung nur überflogen oder nicht beachtet werden. Gefährdet sind die User, die leichtfertig und vorschnell jedes „OK“ anklicken (vgl. Scheffbuch: Teurer Flirt im Netz, 2002, S. 37). Laut polizeilichen Beobachtungen kann behauptet werden, dass die Motivation von jugendlichen Internetnutzern das Auffinden spannender PC-Spiele, Download-Programme, MP3-Files, etc. ist (mündliche Mitteilung von Kriminaloberkommissar Wolfram Künkele vom 2002-07-31). Der Besuch auf umstrittenen Websites ist dadurch eher zu erwarten. Zwischen die gängigen Hinweisfenster der Download-Bestätigung lässt sich geschickt das Programm der Dialer-Software mit einbauen.

Zur Zielgruppe der 0190-Abzocker zählen auch User, die sich oft in Chat-Kanälen aufhalten, und das Internet als eine Plauderecke ansehen. Im Kreise vermeintlich Gleichgesinnter werden vertrauliche und private Unterhaltungen geführt und nicht an eine annähernde Bedrohlichkeit gedacht. „Dort... schlafen wohl die Schutzreflexe“ (Test: Nepp mit 0190, 2002, S. 33). Der Lockruf oder die Empfehlung eines Chat-Partners führt über

einen im Chat zur Verfügung gestellten Link auf die vermeintliche Website, durch die sich der Dialer aktivieren kann.

Wie hoch jedoch die Sensibilisierung der 0190-Problematik bei den Internetnutzern bereits ist (Oktober 02), zeigen verschiedene Presseartikel in allgemeinen Publikumszeitschriften. Das Thema 0190 wird längst nicht mehr nur in einschlägigen Computerzeitschriften oder Fachzeitschriften behandelt, sondern wird auch in Gesundheits-, Fernseh-, Frauen-, Boulevardzeitschriften, u. a. aufgegriffen. Diese Erkenntnis konnte durch einen stichprobenhaften Test durch das Zeitschriftenangebot in der Stadtbibliothek Reutlingen nach Artikeln über 0190-Dialer gewonnen werden. Der Test fand am 2002-08-07 statt, nachdem der Gesetzesänderung der Telekommunikations-Kundenschutzverordnung vom Kabinett zugestimmt wurde (vgl. Kap. 4.4).

4.6 Verhaltensvorschläge

Das Anwachsen der Betrugsfälle durch Internet-Kriminelle ist auf die aktive Mitarbeit der Internetnutzer zurückzuführen. Durch die Bestätigung der kriminellen Machenschaften werden immer wieder neue, raffinierte Dialer-Köder kreiert, die es zu testen durch die Opfer gilt. Mit Beachtung einiger Grundregeln liesse sich dies verhindern. Schutz- und Sicherheitseinstellungen des Rechners rücken durch die Popularität der 0190-Dialer verstärkt in das Bewusstsein der Internetnutzer. Durch die großflächige Zielgruppenansprache dieser Art von Abzocke wird in den Usern Aufmerksamkeit und Unbehagen geweckt, da es schließlich nicht nur um Datenveränderung, sondern um das eigene Geld geht. Die Empfindlichkeit bei eventuell eigenen finanziellen Schäden fördert das Verständnis für die Problematik. Zwar sind Computerviren mittlerweile als potentielle Gefahr für die Datenbestände des eigenen Rechners bekannt, solange keine offensichtlichen Schäden auftreten, werden die angeratenen Sicherheitsvorkehrungen und Verhaltensvorschläge fahrlässig ignoriert.

Die 0190-Welle bringt vor allem bei den gelegentlichen Internetnutzern eine Veränderung der Auffassung über den Schutz persönlicher Daten im Internet mit sich. Die Auseinandersetzung mit PC-Sicherheit ist nicht mehr länger nur Aufgabe von Unternehmen, Behörden, Instituten, Universitäten, etc. Die breite Masse der Internetnutzer ist ange-regt, sich um die Datenbestände Sorgen zu machen. Da keine große Erfahrung mit Computersicherheit von Privatpersonen und kleinen Unternehmen, die keinen System-administrator haben oder sich keinen Sicherheitsfachmann leisten können, zu erwarten

ist, muss Aufklärungsarbeit betrieben werden. Das Interesse für Sicherheitsfragen ist durch die 0190-Abzocke gestiegen. Viele User fühlen sich relativ sicher, wenn auf ihrem System ein veralteter Virens Scanner läuft und/oder sie eine Personal Firewall installiert haben (vgl. hacker's guide, 2001, S. 230).

Die Installation einer Firewall²⁸ und aktuelle Antivirenprogramme können zwar vor Viren und Trojanern schützen, zur Unterlassung von Vorsicht und Aufmerksamkeit beim Surfen wird dennoch nicht geraten. Die Firewall ist kein Freischein für unbekümmertes Surfen. Das unüberlegte Öffnen einer durch E-Mail zugesandten Website oder das unachtsame Bestätigen von Hinweisen sollte tunlichst vermieden werden. Als Schutz vor dem unbemerkten Download eines Dialers können sogenannte 0190er-Warner²⁹ empfohlen werden, die als Free- oder Shareware entweder aus dem Internet heruntergeladen werden können oder auf Begleit-CD's von Computerfachzeitschriften angeboten werden. Diese kleinen Warnprogramme erkennen sowohl Dialer-Programme, die sich bereits auf der Festplatte befinden als auch Dialer, die sich vom Internet aus unbemerkt installieren wollen.

Damit der Internetanschluss nicht zur Kostenfalle wird, sind wenige Grundregeln zu beachten. Diese Sicherheitsvorschläge richten sich ausschließlich an Internetnutzer, die mittels Modem und DFÜ-Verbindung über die Telefonleitung vom Dienst des Internets Gebrauch machen. Im folgenden werden die Sicherheitseinstellungen am PC näher beleuchtet. Allgemeine Vorkehrungen wurden bereits im oberen Abschnitt erwähnt. In kurzer, pragmatischer Weise wird die Handhabung mit dem 0190-Problem im folgenden dargestellt, und ähnelt einer Gebrauchsanweisung.

Durch die Interneteinwahl über das DFÜ-Netzwerk lassen sich Verbindungen zu bestimmten Anbietern gezielt anwählen. So kann verhindert werden, dass durch die Direktwahl über den Browser (Internet Explorer, Netscape Navigator) teure Nummern,

²⁸ Definition Firewall: Eine Firewall stellt eine elektronische Sicherheitsbarriere dar, die Außenstehende, vor allem Hacker davon abhalten soll, auf einen Server oder in ein Netzwerk einzudringen. Der Name leitet sich von Brandschutzmauer ab, die zwischen Häuser errichtet wird und im Brandfall ein Übergreifen der Flammen verhindern soll. Firewalls filtern möglicherweise schädliche Datenpakete aus dem Datenverkehr heraus, und schützen das System vor elektronischen Angriffen und unautorisierten Verbindungen. Als Standardeinstellung ist die Zugriffsverweigerung für verschiedenste Trojaner konfiguriert. Eine Firewall kann hard- und softwarebasiert sein. Personal Firewalls können einzelne PCs effektiv schützen (vgl. Gieseke: Anti-Hacker-Report, 2002, S. 583).

²⁹ In Anhang B.2 sind einige URLs von Dialerschutzprogrammen aufgeführt.

die von dem Dialer als Standardverbindung³⁰ im Browser eingetragen wurden, ausgewählt werden. Das DFÜ-Netzwerk wird aufgerufen über *Arbeitsplatz – DFÜ-Netzwerk*. Darin aufgelistet sind die verschiedenen Einwahlnummern, unter denen sich auch die Dialer-Nummer befinden würde. „Markant sind 0190-Einwahlnummern und Namen für den Internetzugang wie xxxChat, Chatzugang, Hackertools, LiveCam, FlirtLine, ts-cash oder 5-4-30-35 (oder ähnlich)“ (Test: Nepp mit 0190, 2002, S. 33). Zusätzlich ist mindestens ein sichtbares, wenn möglich auch akustisches Signal der bestehenden DFÜ-Verbindung in der Statusleiste hilfreich. Eine Kontrolle über bestehende Verbindungen ist dann gewährleistet. Zusätzlich sollte ein akustisches Signal die Änderung einer DFÜ-Verbindung melden. Das Beenden des Browsers über X (rechts oben) beendet die Internetsitzung nicht zuverlässig sicher. Eine sichere Methode ist das Beenden über das Symbol der DFÜ-Verbindung in der Statusleiste (mit rechter Maustaste *Trennen*). Die Empfehlung, die Internetsitzung durch Ziehen des Netzsteckers abubrechen, sollte nicht als patente Lösung angesehen werden (vgl. Scheffbuch: Teurer Flirt im Netz, 2002, S. 37).

Für die Beweissicherung im Falle einer Strafanzeige ist die vollständige 0190-Nummer herauszufinden. Ein Bildschirmausdruck oder Bildschirmfoto (Screenshot) der besuchten Website und des DFÜ-Verzeichnis dienen den Ermittlungen beim Auffinden des Dialer-Anbieters.

Den zuverlässigsten Schutz vor Dialern bietet die Sperrung der 0190-Nummer von der Telefongesellschaft. Der Gefahr, sich einen Dialer einzufangen, wird damit langfristig entgegengewirkt. Allerdings können andere nützliche und seriöse Servicedienste mit 0190 nicht mehr abgefragt werden, beispielsweise die Rechtsauskunft bei den Verbraucherzentralen oder die Stiftung Warentest.

Durch die Installation eines Schutzprogramms (0190-Warner) werden eingenistete Wählprogramme beseitigt und Installationsversuche neuer Dialer abgewehrt (Angaben zu aktuellen Schutzprogrammen vgl. Anhang B.2). Die Telekom erstellt auf Anforderung einen unverschlüsselten Einzelverbindungs nachweis. So lassen sich auf der Telefonrechnung Verbindungen zu bewusst oder unbewusst angewählten 0190er-Nummern aufzeigen. Eine Kombination aus den Abwehrstrategien Vorsicht beim Surfen, hohe

³⁰ Diese Einstellung kann mit dem Pfad *Start-Einstellungen-Systemsteuerung-Internetoptionen-Verbindungen* verändert werden.

Sicherheitseinstellungen³¹ und ein aktuelles Schutzprogramm sind die Grundlage für die Vermeidung von hohen Telefonrechnungen.

Aus eigener Erfahrung und Äusserungen aus dem persönlichen Umfeld finden die Vorschläge in der Praxis wenig Anwendung. Kaum ein Internetnutzer reagiert im Sinne der Beweissicherung, sondern versucht auf schnellstem Wege den Eindringling wieder zu entfernen.

„Jeder, der im Internet surft, kann durch ein Wählprogramm ‚Dialer‘ ruiniert werden. Wir empfehlen: Strenge Sicherheitseinstellungen: ActiveX und Java deaktivieren. Jedoch sind Funktionseinschränkungen beim Surfen die Folge. Kontrollieren Sie beim Surfen das DFÜ-Netzwerk. Ein aktuelles Schutzprogramm installieren (unter anderem bei www.dialerschutz.de zu finden). Downloads ablehnen, die Ihnen ungefragt aufge-drängt werden. Telefonrechnung kürzen: Bezahlen Sie nur das, was Ihrer Telefongesellschaft zusteht. Widersprechen Sie dem strittigen, von einem Dialer verursachten Betrag... verwenden Sie einen sicheren und schnellen DSL-Zugang“ (Test: Nepp mit 0190, 2002, S. 33).

³¹ Sicherheitseinstellungen des Internet Explorers werden über den Pfad *Extras-Internetoptionen-Sicherheit-Standardstufe* geändert. Mindestens die mittlere Sicherheitsstufe sollte eingestellt sein (vgl. Test: Nepp mit 0190, 2002, S. 33).

5 Abzocker

„Online-Betrug ist vergleichsweise einfach. Abzocker lauern bequem wie die Spinne im Netz auf Opfer“ (Jutzi: Nepper, Schlepper, Surferfänger, 2001, S. 106).

5.1 Abzocker und Nachahmer des kriminellen Geschäftes

Abzocker = Personen, die meist durch Verschleierung der wahren Identität ein kriminelles Verfahren anwenden, um finanzielle Gewinne zu erzielen. Dabei wird i. d. R. ein Geschäftsabschluß (Verkauf von Ware oder Dienstleistung, Tauschgeschäft, etc.) vorgetäuscht, bei dem die versprochene Leistung nicht oder nur zum Teil eingehalten wird. Eine Person, die abgezockt wird, erleidet finanziellen Schaden. Abzocker im Internet verwenden das Internet für organisierten Betrug und täuschen die virtuellen interessierten Geschäftspartner mit angeblichen Leistungen oder Gewinnmöglichkeiten. Vorgestellt wurden diese Betrugsformen an den Beispielen Nigeria Connection und 0190-Dialer³².

Eine Erkenntnis der Untersuchung der Nigeria-Briefe ist das Anpassen der Bittgesuche an tatsächlich geschehene wirtschaftliche, politische und gesellschaftliche Begebenheiten. Im Verlauf der Diplomarbeit ging die Nachricht der Zwangsenteignungen weißer Farmer in Simbabwe durch die Presse (August 02). Ein auffällig großer Anstieg der Angebotsschreiben mit inhaltlichem Bezug auf die Situation der Enteignungen konnte im selben Monat festgestellt werden. „Simbabwe ... ist heute ein heruntergewirtschafteter, von [Präsident Robert] Mugabe autoritär regierter Staat“ (Spiegel Almanach, 1999, S. 489). Das Ziel der vor zwei Jahren gestarteten Landreform ist die Übertragung der von weißen Siedlern bewirtschafteten Farmen auf besitzlose schwarze Landarbeiter, die durch militante Einsätze durchgesetzt werden (vgl. Strauch: Enteignungen in Simbabwe, 2002, <http://www.spiegel.de/politik/ausland/0,1518,210469,00.html>). In den Angebotsschreiben schildern angebliche schwarze Farmer aus Simbabwe die Ermordung des eigenen Vaters, der gegen jene Landreform ebenfalls aufbegehrt hat, und als Vorsichtsmaßnahme sein Vermögen nach Johannesburg gebracht hat.

³² Überblick der bekanntesten Abzocker-Methoden in Kap. 2

Der Sohn lebe nun in den Niederlanden und bittet den Transfer des Geldes ins Ausland zu unterstützen (vgl. Kap. 3.6). 23% der für den Untersuchungszeitraum zur Verfügung stehenden Nigeria-Briefe beinhalten das Anliegen eines schwarzen Farmers aus Simbabwe. Fast 70% der Farmer-Briefe sind im August verschickt worden.

Eine mittlerweile gängige Form von virtuellen Geschäftsbeziehungen sind Internetauktionen - das bekannteste Portal ist „ebay“³³. Das Ausnutzen solcher Internet- oder auch Online-Auktionen stellt eine weitere Variante der zahlreichen Versuche von Vorauszahlungsbetrug unter Verwendung des Neuen Mediums Internet dar. Die Beschreibung der Funktionsweise der Internet-Auktionen führe zu weit und wird im Rahmen der Diplomarbeit nicht behandelt. Es soll vielmehr darauf hingewiesen werden, dass populäre Plattformen für kriminelle Machenschaften benutzt werden und speziell diese Betrugsform bereits zu einer Massenerscheinung von virtueller Kriminalität geworden ist. Die Grundidee von Internet-Auktionen ist das Anbieten von Waren von Internetnutzern für Internetnutzer und deren anschließende Versteigerung. Dabei muss es sich nicht um Personen handeln, die von Berufs wegen im Handelsgewerbe tätig sind. Vorauszahlungen für ersteigerte Ware sind üblich. An dieser Stelle der Geschäftsbeziehung setzt die Betrugsform der Abzocke ein. Der Käufer der ersteigerten Ware tätigt oft eine zu hohe Vorauszahlung. Er wird für Waren zur Kasse gebeten, die nie bei ihm ankommt. In einem Fall in Reutlingen wurden statt der ersteigten DVD-Player alte Autoreifen mit der Post geliefert (mündliche Mitteilung von Kriminaloberkommissar Wolfram Künkele vom 2002-07-31).

Die Teilnehmer an Internetauktionen sind vertrauensseliger als im realen Geschäftsverkehr. Da die Bereitschaft der Internetnutzer für Vorauszahlungen in der virtuellen Geschäftswelt vorhanden ist, konnten sich Betrüger auf deren Kosten problemlos etablieren. Das Vertrauen in den virtuellen Dienstleistungs- oder Warenanbieter wird durch gezielte, werbewirksame Mittel gewonnen. Angebote, Preisreduzierungen, Sonderangebote oder Schnäppchen lassen die Vernunft und den Verstand bei den Internetkunden vorübergehend vergessen. Eine zeitliche Begrenzung setzt den User zusätzlich unter Druck (dieses Versicherungsangebot gilt aber nur noch heute). Das taktisch kluge Vorgehen der Abzocker zahlt sich aus. Auf dem ersten Platz der gesamten Cyber-Kriminalität steht der Betrug mit Online-Auktionen (vgl. Spiegel: Grand Prix der Web-Betrüger, 2002, <http://www.spiegel.de/netzwelt/netzkultur/0,1518,197470,00.html> und

³³ URL: <http://www.ebay.de>, Zugriff am 2002-09-12.

Kap. 2). Nachvollziehbar ist die Teilnahme bei Internet-Auktionen. Kaum eine vergleichbare Alternative für den Erwerb von durchaus günstiger Ware bietet sich dem Verbraucher. Ohne Angebote und Schnäppchen würde die Unternehmensphilosophie eines Internet-Auktions-Portals nicht durchsetzbar sein. Kunden werden schließlich mit den billigen Angeboten angelockt. Die Kontrolle über die Teilnehmer liegt nicht nur in den Händen des Portalanbieters, sondern auch an den Teilnehmern selbst. Bei Warenbetrug über Internet-Auktionen sind bei der überwiegenden Zahl der angezeigten Fälle die Personalien des Täters oder zumindest die Bankverbindung bereits bekannt. Eine rechtliche Belangung im Bereich Internet-Auktionen ist öfters realisierbar als vergleichsweise der Betrug mit den 0190-Dialern (mündliche Mitteilung von Kriminaloberkommissar Wolfram Künkele vom 2002-07-31).

Um den eigenen Geldbeutel zu schützen und den Webganoven das Handwerk zu legen, sollte im Netz die gleiche Vorsicht angewendet werden wie im Alltag. Für den Erwerb von Waren über Online-Auktionen ist auf besondere Vorkehrungen der Auktionshäuser zu achten, z.B. Bewertungslisten fungieren als Erfahrungsaustausch von Auktionsteilnehmer, und Treuhandkonten, die gezahltes Geld bis zum Warenempfang sicherstellen (vgl. Jutzi: Nepper, Schlepper, Surferfänger, 2001, S. 106).

6 Zusammenfassung und Ausblick

Die in dieser Diplomarbeit vorgestellten Betrugsformen zeigen, dass sich Internet und Internet-Kriminalität als Symbiose verhalten. Dem Eroberungsfeldzug des Internets mit dem WWW darf nicht nur der weltweite Kommunikationsaustausch sondern auch die Geburtsstunde der Abzocker zugeschrieben werden. Mit der Projektion der realen Welt in den virtuellen Raum verschwinden die Kontrollmechanismen. Das Internet ist eine Spielwiese, auf der sich sowohl Internetnutzer als auch Betrüger austoben können.

Jeder Internetnutzer setzt sich der Gefahr eines Betrugsversuches aus. Das Vertrauen gegenüber der virtuellen Geschäftswelt darf nicht größer sein als innerhalb der realen Geschäftsbeziehungen. Die Gutgläubigkeit gegenüber Geschäftspartnern nimmt im Internet zu (mündliche Mitteilung von Kriminaloberkommissar Wolfram Künkele vom 2002-07-31). Durch Verschleierung der eigenen Identität, unwahre Angaben, gefälschte Dokumente, etc, kombiniert mit beeindruckender Raffinesse, Hartnäckigkeit und z. T. erstaunlicher Einfachheit werden die Opfer hinter das Licht geführt. Im Gegensatz zu Hackern, die gezielt nach Sicherheitslücken im Betriebssystem der im Netz angemeldeten Rechner suchen, um Datenspionage, -manipulation und -sabotage zu betreiben, handeln Abzocker aus einem anderen Verlangen: die finanzielle Bereicherung.

Schutzmaßnahmen existieren in hinreichender Form. Handelt es sich um Einschleusung von schädigenden Softwareprogrammen, können sog. Firewalls oder spezielle Überwachungstools diese davon abhalten, sich auf der Festplatte des Internetnutzers zu installieren (vgl. Anhang B.2). Generell gilt beim Surfen durch das Internet: Aufmerksamkeit und eine eher skeptisch-vorsichtige Grundhaltung verhindern das Anwachsen der Betrugsopfer.

Leichtsinnigkeit und Vertrauen sind für kriminelle Abzocker die Bestätigung, diese Machenschaften weiterhin zu betreiben. In den einzelnen Kapiteln Nigeria Connection, 0190-Dialer und Abzocker werden Schutzmaßnahmen und Verhaltensvorschläge vorgestellt. Cyber-Kriminalität wird in den verschiedensten Formen weiterhin existieren und sich wie das Internet auch weiterentwickeln. Eine Eingrenzung der Ausbreitung wird nicht zu verhindern sein, solange es Surfer gibt, die in die Falle der Abzocker treten. Dabei würden allein der gesunde Menschenverstand und zuweilen einfacher Verzicht auf ein verlockendes Angebot ausreichen. Tatsächlich erscheint der einzelne Internet-

nutzer, wenn überhaupt eher von seiner Arglosigkeit (um nicht zu sagen Dummheit) und manchmal von seiner Raffgier gefährdet. Dass sich das Internet als Gefährdung herausstellt, wird von der technikgläubigen Öffentlichkeit schlecht verdaut. Insbesondere im Mutterland der Online-Industrie, den USA, bringen User dem Internet eine annähernd religiöse Verehrung entgegen. Kriminelle Attacken zeigen die Kehrseite des lobgepriesenen Netzes auf (vgl. Müller von Blumencron: Dämonen im Datennetz, 2000, S. 109). Auf Regierungsebene werden zwar Maßnahmen gegen den Missbrauch vertraulicher Datenbestände geschaffen, die Belangung der meist anonymen Internet-Kriminellen ist durch die schwierig praktizierende Kontrollfunktion im Netz oft nicht zu verwirklichen.

Anhang A: Ergänzungen zu Themenblock Nigeria Connection

A.1 Beispiele für typische Nigeria-Briefe

From: usman attah <usmanattah@justice.com>
To: payer@hdm-stuttgart.de
Copies to:
Subject: call for help
Date sent: Tue, 18 Jun 2002 12:51:56 +0200

TEL: 234-1-7753874

FAX: 234-1-7595853

E-MAIL: <usmanattah@justice.com>

Date: 18th june, 2002

Dear sir

I pray this important message meets you in good condition of health, may blessings of God be upon you and your family and grant you the wisdom to understand my situation and how much I really need your assistance.

Before I start let me introduce myself. My name is Mrs. Mariam Abacha the wife of the late and former head of state of Nigeria General Sani Abacha. Since the (strange and unfortunate) death of my husband (may God's mercy be upon him), the government has turned against my family.

At first I thought it was a little vendetta from my husband's enemies but I was wrong. They arrested my only son, old enough to take care of the family and then they frozen all our Bank Account known to them, hoping that we will starve to death.

My family is going through hardship; my son is in jail and the remaining ones and myself are under house arrest. The new elected President Olusegun Obasanjo has seized more than US\$660 million dollars from swiss banks already, and they are still seizing a lot of landed property. All that is remaining now is US\$55.8 Million dollars, and this money has been kept in a place I cannot disclose to you now, until we make personal contact.

We cannot touch this money in Nigeria, for you know we are under house arrest and we are being seriously watched by the government. So after discussing with my son, we agreed that we should send the money to your country using a diplomatic courier service in Nigeria. So this is why we need a foreign partner and your help in particular.

Since you will be the one collecting the package in your country, the money will be shared in three ways, i.e. 20% will be used to invest in your country or company and 20% will be for you, while 60% will be for us.

We also hope you can be trusted and you won't disappoint us. Also confidentiality is extremely important. Once the funds arrive in your country we will require you to send us an invitation letter to visit your country and collect our share. This is not a deal or busi-

ness, it is a cry for help. May God guide you. When you reply please leave your contact details, my personal assistant and friend

USMAN ATTAH, he will speak to you and will relate all your messages to me. Please note: You are not expected to pay any upfront money all expenses will be paid by me. If I dare ask you for any upfront payment stop communicating with me.

And for your information this money is drug free and 100% risk free. Time is against us, so your urgent response is needed.

Above, you will see my direct Fax, Telephone number and E-mail address, you can call or send me a fax message.

May God be with you.

USMAN ATTAH

P.A TO MRS MARIAM ABACHA

Abbildung 2: Beispiel eines Nigeria-Briefes der mitleiderregenden Masche eines Familienangehörigen: Mariam Abacha, Frau eines der korruptesten Politiker Nigerias. Briefe von ihr kommen unter verschiedenen Absendern.

Von: onyemartins [mailto:onyemartins@hotmail.com]

Gesendet: Samstag, 3. August 2002 17:10

An: payer

Betreff: NIGERIAN NATIONAL PETROLEUM COPORATION (NNPC)

WARNING

This E-mail transmission contains trade secrets or privileged, undisclosed or other wise highly confidential information. If you have received this E-mail in error, you are hereby notified that any review, copying or distribution of this message is strictly prohibited. You are advised to forward it whom it is addressed to or please inform me immediately and destroy the original transmittal. Thank you for your co-operation.

NIGERIAN LIQUIFIED NATURAL GAS (NLNG)

(A SUBSIDIARY OF NIGERIAN NATIONAL PETROLEUM COPORATION)

PLOT 128 INDEPENDENCE AVENUE, ABUJA-NIGERIA.

SUBJECT: SIX MILLION (\$6,000,000.00) U.S DOLLARS TRANSFER

ATTN: THE CHAIRMAN/C.E.O

DEAR SIR/MADAM,

THANKS FOR A GOOD PIECE OF INFORMATION I GATHERED ABOUT YOU IN MY QUEST TO GET AN HONEST AND TRUST WHORTHY PERSON FOR THIS BUSINESS TRANSACTION.

I AM DR. MARTINS ONYE, A DIRECTOR GENERAL WITH NIGERIAN LIQUIFIED NATURAL GAS (NLNG). WE HAVE A TOTAL OF \$6,000,000.00 U.S DOLLARS WHICH WE WANT TO TRANSFER TO A FOREIGN BANK ACCOUNT FOR SAVE KEEP AND INVESTMENT. THE MONEY ACRUED AS A RESULT OF OVER INVOICING DURING THE CONSTRUCTION OF THE SECOND PHASE OF THE NLNG PLANT AT BONNY - PORT HARCOURT. HOWEVER, AS CIVIL SERVANT IN NIGERIA, WE ARE NOT ALLOWED TO HAVE FOREIGN BANK ACCOUNT. I WILL OFFER YOU 20% OF THE TOTAL MONEY IF YOU CAN PRODUCE BANK ACCOUNTS WHERE THIS FUND WILL BE TRANSFERRED INTO FOR SAVE KEEP AND INVESTMENT.

IT MAY INTEREST YOU TO KNOW THAT LATE LAST YEAR, I EXECUTED A SIMILAR

TRANSACTION OF THIS NATURE WITH AN OSAKA-JAPAN BASED MULTI MILLIONARE BUSINESS WOMAN MRS KONAMI YAMAMOTO WITH PHONE NUMBER: 81-9085437498. WHEN THE MONEY WAS EVENTUALLY TRANSFERRED INTO HER BANK ACCOUNT IN JAPAN, SHE SUPRISINGLY SEIZED THE WHOLE MONEY WITH OUT REPATRIATING MY OWN SHARE. HENCE, DUE TO THIS PAST TRAUMATIC EXPERIENCE, YOUR HONESTY AND TRANSPARENCY IS OF HIGH DEMAND. HOWEVER, DUE TO STRICT CONFIDENTIAL REASONS, YOU ARE REQUIRED TO REPLY THIS LETTER MY INDICATING YOUR INTEREST THROUGH THIS FAX NUMBER ONLY: 234-9-2726214. YOU ARE ALSO REQUIRED TO STATE YOUR PERSONAL E-MAIL ADDRESS, FAX NUMBER AND PHONE NUMBER IN YOUR FAX REPLY.
THANKS.

YOURS TRULY,
DR. MARTINS ONYE

NOTE: SEND YOUR REPLY THROUGH THIS PRIVATE FAX NUMBER ONLY: 234-9-2726214

Abbildung 3: Beispiel eines Nigeria-Briefes der geschäftlich Masche

Von: LOVEASSEMBLY [mailto:LOVEASSEMBLY@MINISTER.COM]
Gesendet: Mittwoch, 24. Juli 2002 00:00
An: payer
Betreff: YOUR ATTENTION REQUIRED

LOVE OF CHRIST ASSEMBLY
CHURCH EMAIL: loveassembly@minister.com
PRIVATE EMAIL: loveassembly@minister.com
tel: 234-803-3400719

Dear brethren,

I am writing you this letter in view of the fact that we could be of assistance to each other, bringing the riches of the gentiles for good purpose in accordance to the will of the Lord, Most High. Amen.

Firstly, considering the urgency required to ensure success of the transaction I am about to explain to you, I found your email through email list, and considered it a privilege to solicit for your assistance in realizing the business, as I do not have any other contact to realize it.

It is important to note that I am not embarking in this project out of greed, but out of burning desire to do Gods work, through providing charity in accordance with biblical principles to the helpless orphan, and the rejected and dejected disabled people, and also not scam as I have made arrangement to sell the rolex watch of my late master in my custody to send you money to pay all government taxes, transfer charges and necessary fees to support the release of the funds to you. For your security, and the success of this transaction, all the banking will be done securely to prevent undue question by your bank or your country's government due to the amount involved.

I am by name brother Uwom Oluigbo, church assistant and housekeeper to late Rev. Dr. Simon Wood, a foreign missionary nationalized in Nigeria, and president of Love of Christ Assembly, and Outreach for the Poor and the Disabled, being a volunteer, Christian charity organization primarily involved in providing support for the less privileged, handicapped and orphaned children and widows alike.

Late Rev. Dr. Simon Wood received donation from international charity organizations, churches, government corporations, businesses and individuals from all parts of the world to help in providing food, medication, and in provision of skill development and small scale ventures to enable handicapped people to engage in meaningful activities. A total of Eleven million United states dollars (11,000,000 USD) was realized which he (late Rev. Simon) had projected to invest in sustainable agriculture, and multi-fruit processing plant, and self help projects to give life meaning to the handicapped and orphaned people.

Late Rev. Dr. Simon Wood was murdered in the recent bomb explosion, which took place at Ikeja military cantonment (Lagos, Nigeria) ammunition depot affecting the entire Ikeja area, burying houses, and killing thousands of innocent people in different places in Lagos State, Nigeria. Love of God Assembly building collapsed killing many of the disabled people including Rev. Dr. Simon Wood.

Late Rev Dr. Simon Wood was very committed to helping the poor and lived a life of total service for the upkeep of the handicapped and the less privileged. He did not marry, and did not have children. I am the housekeeper and his assistant. He did not make any will and also did not leave information about his relatives. The entire balance of 11 million United States dollars exists in his personal account, which nobody knows about except me, and the news of his death has spread, as he was known to be a friend and hope of the poor and handicapped.

The bankers are honestly waiting for anybody that has correct information who is the next of Kin. You do not need to be a relative to be the next of kin to late Rev. Dr. Simon Wood.

I have worked out perfect arrangement that is safe and quick to enable us claim the funds, because if we do not the corrupt government officials will divert the fund to private purses and never for any orphan or handicapped person. Nigerian government is very corrupt and indifferent to the poor and helpless people. Please verify these facts.

I will offer you 20 percent for assistance, 5 percent for settlement of any expenses incurred during the transfer period, 40 percent will be used later to found my own charity organization to continue for the physically handicapped and 35 percent for my private use (of which 10 percent of my own share will be given as tithe in accordance with biblical teachings).

If you are interested, please contact me immediately so that we can proceed with arrangements.

Treat this as very urgent.

Please reply to the email address:
CHURCH EMAIL: loveassembly@minister.com
PRIVATE EMAIL: loveassembly@minister.com

PLEASE NOTE I WILL BEAR ALL COSTS. I DO NOT NEED ANY MONEY FROM YOU. SHOULD. I ASK YOU FOR ANY MONEY IN ADVANCE PLEASE REPORT ME TO FBI OR THE SECURITY SERVICE OF YOUR COUNTRY.

Brother Uwom Oluigbo

Please visit the websites below to obtain full information about the bomb explosion in Nigeria.

http://news.bbc.co.uk/hi/english/talking_point/newsid_1787000/1787000.stm
<http://www.vanguardngr.com/news/articles/2002/January/29012002/f4290102.htm>

Abbildung 4: Beispiel eines Nigeria-Briefes der frommen Masche

Von: david nkroma [mailto:davidnkroma_2@lycos.com]
Gesendet: Montag, 12. August 2002 12:46
An: [mailto:davidnkroma_2@lycos.com]
Betreff: Soliciting Your Assistance.

DAVID NKROMA,
AMSTERDAM THE NETHERLANDS
TEL:0031 613 777 023.

CONFIDENTIAL PROPOSAL

You may be surprised to receive this letter from me since you do not know me personally. The purpose of my introduction is that I am David Nkroma, the first son of Mandi Nkroma, one of the most popular black farmers in Zimbabwe who was recently murdered in the land dispute in my country. Before the death of my father, he had taken me to Johannesburg to deposit the sum of US4.5 million four million, Five Hundred thousand United States dollars, in one of the private security company, as he foresaw the looming danger in Zimbabwe this money was deposited in a box as gem stones to avoid much demurrage from security company. This amount was meant for the purchase of new machines and chemicals for the Farms and establishment of new farms in Swaziland.

This land problem came when Zimbabwean President president Robert Mugabe introduced a new Land Act Reform wholly affecting the rich white farmers and some few black farmers, and this resulted to the killing and mob action by Zimbabwean war veterans and some lunatics in the society. In fact a lot of people were killed because of this Land reform Act for which my father was one of the victims.

It is against this background that, I and my family fled Zimbabwe for fear of our lives and are currently staying in the Netherlands where we are seeking political asylum and moreso have decided to transfer my father's money to a more reliable foreign account. since the law of Netherlands prohibits a refugee (asylum seeker) to open any bank account or to be involved in any financial transaction throughout the territorial zone of Netherlands. As the eldest son of my father, I am saddled with the responsibility of seeking a genuine foreign account where this money could be transferred without the knowledge of my government who are bent on taking everything we have got. The South African government seems to be playing along with them.

I am faced with the dilemma of moving this amount of money out of South Africa for fear of going through the same experience in future, both countries have similar political history. As a businessman, I am seeking for a partner who I have to entrust my future and that of my family in his hands, I must let you know that this transaction is risk free. If you accept to assist me and my family, all I want you to do for me, is to make an arrangements with the security company to clear the consignment(funds) from their affiliate office here in the Netherlands as i have already given directives for the consignment to be brought to the Netherlands from South Africa. But before then all modalities will have to be put in place like change of ownership to the consignment and more importantly this money I intend to use for investment.

I have two options for you. Firstly you can choose to have certain percentage of the money for nominating your account for this transaction. Or you can go into partnership with me for the proper profitable investment of the money in your country. Whichever the option you want, feel free to notify me. I have also mapped out 5% of this money for all kinds of expenses incurred in the process of this transaction. If you do not prefer a partnership I am willing to give you 10% of the money while the remaining 85% will be for my investment in your country. I shall await your response while I implore you to maintain the absolute secrecy required in this transaction.

Thanks, GOD BLESS YOU

Yours Faithfully,

David Nkroma.

Abbildung 5: Brief eines angeblichen schwarzen Farmers aus Simbabwe in Nachahmung der Nigeria-Briefe

A.2 Liste der Absender der Nigeria-Briefe

- | | |
|-----------------------|-------------------------|
| 1. Abacha, Abdulkadir | 44. Maikudi, Abdulrasaq |
| 2. Abacha, Habib | 45. Maki, Atu |
| 3. Abacha, Mariam | 46. Malamba, Peter |
| 4. Adebayo, David | 47. Mambo, Sani |
| 5. Ahmed, Saeed | 48. Masarah, David |
| 6. Alameyah, Idris A. | 49. Mello, Eduardo de |
| 7. Alli, Kaloma | 50. Merimbe, Nkala |
| 8. Audu, Jonathan | 51. Momoh, Dumen |
| 9. Awka, Nwaokoye | 52. Mowete, Johnson |

- | | |
|---------------------------|---------------------------------|
| 10. Bako, Danladi | 53. Moyo, Dickson |
| 11. Bamti, Kalua | 54. Moyo, GeorgeMusa, Ali |
| 12. Bashir, Ali Baba | 55. Mulete, Edward |
| 13. Bello, Isa | 56. Nana, Philipps |
| 14. Bello, Yaya | 57. Nkomo, Ajala |
| 15. Benselah, Vincent | 58. Nkroma, David |
| 16. Bunmi, Uwa | 59. Ntobo, Lauren |
| 17. Chidi, Augustine | 60. Nzaga, Michael |
| 18. Cole, Dele | 61. Obaro, Joseph |
| 19. Colins, Joseph | 62. Obi, Ifeanyi |
| 20. Dilet, Jacques | 63. Obulu, Obidike |
| 21. Douglas, Seleck | 64. Oki, Richard |
| 22. Duke, Philipps | 65. Oluigbo, Uwom |
| 23. Duru, Henry | 66. Onye, Martins |
| 24. Edward, Joseph | 67. Peters, Amadi |
| 25. Elue, Augustus | 68. Pius, Owode |
| 26. Emeifiele, Godwin | 69. Robert, Nkono |
| 27. Fashola, Benjamin | 70. Savimbi, David |
| 28. Fernandez, Kola | 71. Sandox, Emmanuel |
| 29. Fuma, Roseline | 72. Sangala, Ashton |
| 30. Guei, James | 73. Saro-Wiwa, Patience |
| 31. Isoko, Steven | 74. Savimbe, Joachim |
| 32. John, Mbezi | 75. Savimbi, Joseph |
| 33. Johnson, Ericmanuel | 76. Savimbi, Sandra |
| 34. Jones, Segun | 77. Sese-Seko, Jean-Paul Thiong |
| 35. Jos, Mamman | 78. Sese-Seko, Kalisara |
| 36. Kabila, Beatrice | 79. Sese-Seko, Mariam |
| 37. Kabila, Laurent Mpeti | 80. Sese-Seko, Nguema Mobutu |
| 38. Kabila, Tutu | 81. Tambo, Zuma |
| 39. Kadiri, Abdul | 82. Taytaie, Johnson |
| 40. Kargbo, Daniel | 83. Udogwu, Nkadi |
| 41. Kebba, Michael | 84. Umar, Abdulrazak |
| 42. Khumalo, Bram | 85. Uyi, Osaro |
| 43. Mabutu, Sadebe | 86. Williams, Olawale |

Abbildung 6 : Liste mit Absendern der Nigeria Connection im Untersuchungszeitraum [einige haben wiederholt Briefe geschickt]

Anhang B: Adressen und spezielle Informationen für Angeschriebene, Geschädigte und Interessenten

B.1 Nigeria Connection

Im Internet unter

http://www.auswaertiges-amt.de/www/de/laenderinfos/419_html,

<http://www.internet.bap.admin.ch/d/aktuell/warnung/n-betrueger.htm>,

http://www.polizei-bw.de/fahndung/warmeldung/warmmeldungen_nigeria.htm,

<http://www.fraud.org/tips/internet/nigerian.htm>,

http://www.quatloos.com/cm-niger/nigerian_scam_letter_muse_um.htm [Auf der Website einer amerikanischen Finanzberatungsorganisation werden in einer Galerie über 100 Nigeria-Briefe gezeigt], u. a.

Adresse der für Deutschland
zuständigen Vertretung:

Botschaft der Bundesrepublik Nigeria Platanenstraße 98a, 13156 Berlin

Tel. 030 – 477 23 00/ - 01

Fax 030 – 477 25 55

Adressen der deutschen Vertretungen:

Botschaft der Bundesrepublik Deutschland Plot 433, Yakubu Gowon Crescent (opposite ECOWAS Secretariat), Asokoro District, Abuja FCT, Abuja

Tel. 00234 9 – 314 80 05

Fax 00234 9 – 314 80 06

E-Mail asgeremb@hotmail.com

Postanschrift: Embassy of the Federal Republic of Germany Abuja, P. M. B. 280, Garki, Abuja FCT, Nigeria

Außenstelle der Botschaft der Bundesrepublik Deutschland in Abuja

15 Walter Carrington Crescent (formerly Eleke Crescent), Victoria Island, Lagos, Nigeria

Tel. 00234 1 – 261 10 82

Fax 00234 1 – 261 11 73

e-mail gembassylagos@micro.com.ng

Postanschrift: Embassy of the Federal Republic of Germany – Embassy Office in Lagos, P. O. Box 72800, Victoria Island, Lagos, Nigeria

[Quelle: Auswärtiges Amt: Länder- und Reiseinformationen ; Nigeria. -- URL:
http://www.auswaertiges-amt.de/www/de/laenderinfos/vertretungen/ausl_vertretung?land_id=125. -- Zugriff am 2002-10-04, URL: http://www.auswaertiges-amt.de/www/de/laenderinfos/adressen/dtl_vertretung?land_id=125. -- Zugriff am 2002-10-04]

B.2 0190-Dialer

Im Internet unter

<http://www.regtp.de>,

<http://www.fst-ev.org>

aktuelle Tipps und Hinweise zu Schutzsoftware

<http://www.dialerhilfe.de>,

<http://www.dialerschutz.de> [das Schutzprogramm YAW, Version 3.01 wehrt den Versuch der Wählerprogramme ab, solche Schutzprogramme abzuwehren],

<http://www.idi.de>,

<http://www.internetfallen.de>,

<http://www.trojaner-info.de>, u. a.

Nach einem Artikel aus der Stuttgarter Zeitung rät die Industrie- und Handelskammer Region Stuttgart ungerechtfertigten Telefonabrechnungen schriftlichen Widerspruch einzulegen bei

Telekommunikationsbehörde

Beschwerdemanagement

Postfach 44 01 62

80750 München

[Quelle: Telefonkosten im Zweifel anfechten. -- In: Stuttgarter Zeitung online. -- Fassung 2002-08-14. -- URL: <http://www.stuttgarter-zeitung.de/stz/page/detail.php/240587>. -- Zugriff am 2002-08-26]

Literatur- und Quellenverzeichnis

Afemann: Internet für Entwicklungsländer, 2001

AFEMANN, UWE: „E-velopment“ : Vor- und Nachteile des Internet für Entwicklungsländer. -- Fassung vom 2001-08-15. -- URL: http://www.home.uni-osnabrueck.de/uafemann/Internet_Und_Dritte_Welt/AsienBerlin.htm. -- Zugriff am 2002-09-23

Ahlf: Korruption, 1998

AHLF, ERNST-HEINRICH: Korruption. – Hilden : Verlag Deutsche Polizeiliteratur, 1998. – 72 S. – (Lehr- und Studienbriefe Kriminologie ; Nr. 13). – ISBN 3-8011-0391-9

Auswärtiges Amt: Hinweise Nigeria-Connection, 2002

Auswärtiges Amt: Länder- und Reiseinformationen : Nigeria-Connection -- Hinweise zum sogenannten Vorauszahlungsbetrug „Nigeria-Connection“ („419-Connection“). -- Fassung vom 2002-06-19. -- URL: http://www.auswaertiges-amt.de/www/de/laenderinfos/419_html. -- Zugriff am 2002-07-17
[gute, verständliche Kurzbeschreibung des Betruges der Nigeria Connection]

BKA: Polizeiliche Kriminalstatistik, 2001

BKA: Polizeiliche Kriminalstatistik : Computerkriminalität ; Berichtsjahr 2001. -- URL: <http://www.bka.de/pks/pks2001/index2.html>. -- Zugriff am 2002-09-20

BOTTI, GIUSEPPE: Betrüger : Nigeria-Connection plündert Sparkonto. – In: Beobachter. – 2001-08-31, Nr. 18. – S. 24

Computerwoche: Schutz vor 0190-Abzocke, 2002

Gesetzesänderung geplant : Regierung will Schutz vor 0190-Abzocke verbessern. – In: Computerwoche. – (2002), Nr. 24. – S. 8

Cremer: Korruption begrenzen, 2000

CREMER, GEORG: Korruption begrenzen : Praxisfeld Entwicklungspolitik. – Freiburg i. Br. : Lambertus, 2000. – ISBN 3-7841-1289-7. –
Zitiert nach: Payer, Margarete: Internationale Kommunikationskulturen. -- 8. Kulturelle Faktoren: Bürokratie und Korruption. -- 3. Teil III: Korruption. -- Fassung vom 2001.03-05. -- URL: <http://www.payer.de/kommkulturen/kultur083.htm>. -- Zugriff am 2002-09-05

CZIESCHE, DOMINIK: Geködert und geprellt / von Dominik Cziesche; Andrea Stuppe. – In: Der Spiegel. – 2002-05-18, Nr. 21. – S. 44

DIEZEMANN, ECKART: Nigeria. – 2. überarb. Aufl. – Pforzheim : Goldstadtverlag, 1992. – 299 S. : zahlr. Fotos - (Goldstadt-Reiseführer ; Band 204). – ISBN 3-87269-204-6
[illustrierter Reiseführer mit Farbfotos und praktischen Reisetipps]

Eimeren: ARD/ZDF-Online-Studie, 2002

EIMEREN, BIRGIT VAN: ARD/ZDF-Online-Studie2001 : Internetnutzung stark zweckgebunden ; Entwicklung der Onlinemedien in Deutschland / von Birgit van Eimeren; Heinz Gerhard; Beate Frees. – In: Media Perspektiven. - (2001), Nr. 8. – S. 382-397. –
Online unter: http://www.ard-werbung.de/showfile.phtml/2001_08_01.pdf?foid=2.

FAZ: BKA warnt, 1995

BKA warnt vor der „Nigeria-Connection“ : Deutsche Geschäftsleute wurden um 40 bis 60 Millionen DM betrogen. – In: Frankfurter Allgemeine Zeitung. – 1995-04-29. – S. 18

Fischer: Computer-Kriminalität, 1979

FISCHER, THOMAS: Computer-Kriminalität : Gefahren und Abwehrmassnahmen. – Bern: Verlag Paul Haupt, 1979. – 43 S. - (Betriebswirtschaftliche Mitteilungen ; Nr. 71). – ISBN 3-258-02884-2

Fischer Weltalmanach, 2002

BARATTA, MARIO VON (Hrsg.): Der Fischer Weltalmanach. – Frankfurt am Main : Fischer Taschenbuch Verlag, 2002. – ISBN 3-596-72002-8

FIUTAK, MARTIN: Regierung verabschiedet Dialer-Gesetz. -- Fassung vom 2002-07-31. -- URL: <http://news.zdnet.de/sory/0,,t101-s2120120,00.html>. -- Zugriff am 2002-08-03

Galtung: Zum Beispiel Korruption, 1994

GALTUNG, FREDERIK: Eine Koalition gegen die Bestechlichkeit. – In: Zum Beispiel Korruption / Redaktion: Frederik Galtung. – Göttingen : Lamuv, 1994. – (Lamuv-Taschenbuch ; 158) (Süd-Nord). – ISBN 3-889-77371-0. -

Zitiert nach: Payer, Margarete: Internationale Kommunikationskulturen. -- 8. Kulturelle Faktoren: Bürokratie und Korruption. -- 3. Teil III: Korruption. -- Fassung vom 2001.03-05. -- URL: <http://www.payer.de/kommkulturen/kultur083.htm>. – Zugriff am 2002-09-05

Gea: Kriminelle aus Nigeria, 1996

„Nigeria-Connection“ läßt nicht locker : Kriminelle aus Nigeria in Baden-Württemberg zunehmend aktiv. – In: Reutlinger General-Anzeiger. – 1996-01-04. – Kopie des Artikels aus Archiv des Reutlinger General-Anzeigers ohne Seitenzahl

Gerny: Via Lagos, 1994

GERNY, DANIEL: Via Lagos auf sicherem Weg zum Bankrott. – In: Der Bund. – 1994-09-29. – S. 6

Gieseke: Anti-Hacker-Report, 2002

GIESEKE, WOLFRAM: Anti-Hacker Report. – 1. Aufl. – Düsseldorf : Data Becker, 2002. – 606 S. : zahlr. Ill. – ISBN 3-8158-2218-1

hacker's guide, 2001

Der neue hacker's guide : Sicherheit im Internet und im lokalen Netz. – München : Markt+Technik Verlag, 2001. – 1017 S. – ISBN 3-8272-5931-2
[umfangreiches, pragmatisch geschriebenes Grundlagenwerk zum Thema Internet, Hacker und Sicherheit]

Harenberg Länderlexikon, 1998

Harenberg Länderlexikon. – Dortmund : Harenberg Lexikon Verlag, 1998. – ISBN 3-611-00681-5

Henauer: Betrügerbanden, 2002

HENAUER, MARC: Nigerianische Betrügerbanden : Bundesamt für Polizei, Schweiz. -- Fassung vom 2002-06-04. -- URL: <http://www.internet.bap.admin.ch/d/aktuell/warnung/n-betrueger.htm>. -- Zugriff am 2002-08-29

Hirschbiegel: Zauberlösung, 2001

HIRSCHBIEGEL, THOMAS: Mit „Zauberlösung“ und ganz viel Hokus-Pokus 50 000 Mark abgezockt / von Thomas Hirschbiegel; Olaf Wunder. – In: Hamburger Morgenpost. – 2001-03-16. – S. 20

Internet Fraud Complaint Center IFCC: Statistics : Nigerian Letter Scams Report. -- URL: <http://www1.ifccfbi.gov/index.asp#IFCC>. -- Zugriff am 2002-08-29

Jutzi: Nepper, Schlepper, Surferfänger, 2001

JUTZI, SEBASTIAN: Nepper, Schlepper, Surferfänger : Abzocker entdecken das Netz für ihre Machenschaften. – In: Focus. – 2001-08-06, Nr. 32. – S. 104-106

KALENBERG, CLAUDIA: Verbraucherinformation zu unverlangter Werbung / hrsg. von Freiwillige Selbstkontrolle Telefonmehrwertdienste e. V. -- Fassung vom 2001-12-27. -- URL: <http://www.fst-ev.org/ger/verbraucherinfos/druck/unverlangtefaxundsmswerbung.html>. – Zugriff am 2002-08-29

Körner: Nigeria, 1999

KÖRNER, PETER: Nigeria, der volkreichste Staat des Kontinents. – In: Informationen zur politischen Bildung. – (1999), Nr. 264. – S. 47

Mack: Fax spuckt alte Information, 2002

MACK, DANIELA: Fax spuckt für teures Geld nur alte Informationen aus. – In: Stuttgarter Zeitung. – 2002-08-20, Nr. 192. – S. 17

Mäder: Nigeria-Nepper, 1994

MÄDER, RUEDI: Fintenreiche Nigeria-Nepper suchen Schweizer Deppen. – In: Aargauer Tagblatt. – 1994-10-22 – S. 3-4

Maise: Nigeria-Millionen, 1996

MAISE, FELIX: Wenn Nigeria-Millionen locken. - In: Tages-Anzeiger, Zürich. – 1996-12-28. – S. 10

MANSFIELD, RICHARD: Hacker Attack. – 1. Aufl. – Düsseldorf : Sybex-Verlag, 2001. – 347 S. – ISBN 3-8155-0400-7

MEDOSCH, ARMIN: Netzpiraten : Die Kultur des elektronischen Verbrechens / von Armin Medosch; Janko Röttgers (Hrsg.). – 1. Aufl. – Hannover : Verlag Heinz Heise, 2001 (Telepolis). – 189 S. – ISBN 3-88229-188-5

Müller von Blumencron: Dämonen im Datennetz, 2000

MÜLLER VON BLUMENCRON, MATHIAS: Hacker : Dämonen im Datennetz. – In: Der Spiegel. – (2000), Nr. 7. – S. 108-110

National Consumers League: Nigerian Money Offers : Internet Fraud Tips from the National Consumers League's Internet Fraud Watch. -- URL: <http://www.fraud.org/tips/internet/nigerian.htm>. -- Zugriff am 2002-07-17
[der amerikanische Verbraucherverband gibt Tipps zur Vermeidung von finanziellen Schäden durch die Nigeria Connection]

Nashat: Konflikte in Nigeria, 2002

NASHAT, BIDJAN TOBIAS: Religiöse und politische Konflikte im Vielvölkerstaat Nigeria : „Ruhende Schwangerschaften“ in Tunga Tudú. – In: Anklagen, Amnesty international. – 2002-06-01, Nr. 2. – S. 3

NOHLEN, DIETER (Hrsg.): Handbuch der dritten Welt : Westafrika und Zentralafrika / hrsg. von Dieter Nohlen; Franz Nuscheler. – 3., völlig neu bearb. Aufl. – Bonn : Dietz, 1993. – 559 S. : statistische Tab. – (Handbuch der dritten Welt ; Bd. 4). – ISBN 3-8012-0204-6

NZZ: Afrikas Rache, 2002

Afrikas Rache kommt virtuell : Wie der weisse Mann für den Kolonialismus bestraft wird. – In: Neue Zürcher Zeitung. – Schweizer Ausgabe. – 2002-09-26, Nr. 223. – S. 47

NZZ: FBI engagiert sich für Ethik, 2000

FBI engagiert sich für Ethik. – In: Neue Zürcher Zeitung. – Internationale Ausgabe. – 2000-10-20, Nr. 245. – S. 53

NZZ: Frontenwechsel, 2001

Frontenwechsel eines Generals in Nigeria : ein pensionierter Offizier im Kampf gegen die Korruption. - In: Neue Zürcher Zeitung. - Internationale Ausgabe. - 2001-02-24, Nr. 46. - S. 7. -
Online unter: <http://www.nzz.ch/2001/02/24/al/page-article774YP.html>

PARDEY, HANS-HEINRICH: Der Mann in der Mitte soll an der Brandmauer scheitern. – In: Frankfurter Allgemeine Zeitung. – 1997-05-27, Nr. 120. – S. 41

Poldervaart: Post aus Afrika, 1998

POLDERVAART, PIETER: Teure Post aus Afrika. – In: Basler Zeitung. – 1998-10-09. – S. 18

Polizei Ba-Wü: Trickbetrüger, 2002

Polizei Baden-Württemberg: Warnmeldungen : 0190-Service-Nummer. -- URL: http://www.polizei-bw.de/fahndung/warnmeldung/warnmeldungen_0190.htm. -- Zugriff am 2002-08-26

Polizei Ba-Wü: Warnmeldungen, 2002

Polizei Baden-Württemberg: Warnmeldungen : Nigerianische Betrüger nutzen das Internet. -- URL: http://www.polizei-bw.de/fahndung/warnmeldung/warnmeldungen_nigeria.htm. -- Zugriff am 2002-08-26

Proteste gegen den Regierungsbeschluß zu 0190er Telefonnummern. – In: Frankfurter Allgemeine Zeitung. – 2002-06-20, Nr. 140. – S. 22

RegTP: Informationen 0190-Dialer, 2002

Regulierungsbehörde für Telekommunikation und Post: Informationen zu (0)190-0-Dialer. -- URL: <http://www.regtp.de/service/02501/01/index.html>. -- Zugriff am 2002-08-29
[übersichtliche Einführung zu Dialer, rechtliche Bewertung und Handlungsmöglichkeiten für den Verbraucher]

Schade: Wie mache ich das intelligent?, 1999

SCHADE, THOMAS: „Wie mache ich das intelligent?!“ : Kriminalität im Internet. – In: Sächsische Zeitung. – 1999-01-04, Nr. 2. – S. 3

Scheffbuch: Teurer Flirt im Netz, 2002

SCHEFFBUCH, PHILIPP: Der Flirt im Netz kann teuer werden. – In: Tagesspiegel. – 2002-03-23. – S. 37. –
Online unter: <http://archiv.tagesspiegel.de/archiv/22.03.2002/ak-wi-ve-4418832.html>. - Zugriff am 2002-07-17

SCHUMACHER, JÖRG: Sicherheit im Internet : Gewusst wie! / von Jörg Schumacher; Eike Elser. – München : Markt+Technik Verlag, 2000. – 208 S. : zahlr. Abb. – ISBN 3-8272-5758-1

Scott: Network Security the Wild West, 2001

SCOTT, WILLIAM B.: Network Security still the ‚Wild West‘. – In: Aviation Week. – 2001-02-26, Nr. 9. – S. 62

Spiegel Almanach, 1999

Spiegel Almanach `99 : Alle Länder der Welt ; Zahlen, Daten, Analysen. - Hamburg : Spiegel-Buchverlag und Hoffmann und Campe Verlag, 1999. - 639 S. : zahlr. Ill. – ISBN 3-455-15008-X (Buch mit CD-Rom).
[schneller Einblick über wesentliche Fakten und Zahlen des gewünschten Landes]

Spiegel: Gesetz ist durch, 2002

Das Gesetz ist durch : Regierung verbessert Schutz gegen 0190-Abzocke. -- In: Spiegel Online. -- Fassung vom 2002-08-01. -- URL: <http://www.spiegel.de/netzwelt/politik/0,1518,207650,00.html>. -- Zugriff am 2002-08-26

Spiegel: Grand Prix der Web-Betrüger, 2002

Nepper, Schlepper, Bauernfänger : Grand Prix der Web-Betrüger. -- In: Spiegel online. -- Fassung vom 2002-05-24. -- URL: <http://www.spiegel.de/netzwelt/netzkultur/0,1518,197470,00.html>. -- Zugriff am 2002-08-08

Spindler: Internet-Auktionen, 2001

SPINDLER, GERALD: Internet-Auktionen : Rechtliche Rahmenbedingungen / hrsg. von Gerald Spindler; Andreas Wiebe. -- München : Beck, 2001. -- 357 S. -- ISBN 3-406-47056-4

Stahn: Nigeria, 1995

STAHN, EBERHARD: Nigeria : Reiseführer mit Landeskunde. -- 4. Aufl. , [Neuausg.] 1. Aufl. -- Dreieich bei Frankfurt am Main : Mai's Reiseführer Verlag, 1995. -- 346 S. : zahlr. Fotos -- (Mai's Weltführer ; Nr. 3). - ISBN 3-87936-220-3
[illustrierter Reiseführer mit Informationen zu Land und Leuten, Natur, Kultur und Geschichte samt reisepraktischen Tipps]

Stark: Kriminelle Nigerianer, 2000

STARK, HOLGER: Für Kleinkram sind die kriminellen Nigerianer nicht zu haben : Vor allem im Scheck- und Kreditkartenbetrug ist die „Nigeria-Connection“ tätig. -- In: Tagesspiegel. -- 2000-10-01. - S. 12

Strauch: Enteignungen in Simbabwe, 2002

STRAUCH, RÜDIGER: Enteignungen in Simbabwe : Weiße Farmer leisten Widerstand gegen Diktator Mugabe. -- In: Spiegel online. -- Fassung vom 2002-08-22. -- URL: <http://www.spiegel.de/politik/ausland/0,1518,210469,00.html>. -- Zugriff am 2002-10-04

Test: Nepp mit 0190, 2002

Nepp mit 0190-Wahlprogrammen : 1650 Euro für 33 Minuten. -- In: Test. -- (2002), Nr. 8. -- S. 31-33

Thamm: Mafia global, 1998

THAMM, BERNDT GEORG: Mafia global : Organisiertes Verbrechen auf dem Sprung in das 21. Jahrhundert / von Berndt Georg Thamm; Konrad Freiberg. Unter Mitarb. von Elmar Ruhlich; Jürgen Storbeck. -- Hilden : Verlag Deutsche Polizeiliteratur, 1998. -- 383 S. -- ISBN 3-8011-0354-4

TI: Über TI, 2002

Transparency International Deutsches Chapter e. V.: Wer sind wir? : Über TI. -- Fassung vom 2002-03-19. -- URL: <http://www.transparency.de/html/ueberti.html>. -- Zugriff am 2002-08-26

Troebs: Nigeria-Connection, 1995

TROEBS, HARTMUT: Die „Nigeria-Connection“ ist noch nicht erledigt. -- In: Reutlinger General-Anzeiger. -- 1995-01-28. -- Kopie des Artikels aus Archiv des Reutlinger General-Anzeigers ohne Seitenzahl

Troebs: Nigeria-Connection lauert, 1995

TROEBS, HARTMUT: Nigeria-Connection lauert weiter auf Opfer. -- In: Reutlinger General-Anzeiger. - 1995-04-28. - Kopie des Artikels aus Archiv des Reutlinger General-Anzeigers ohne Seitenzahl

Vosseberg: hackerz book, 2002

VOSSEBERG, THOMAS: hackerz book : so greifen hacker pc's an. – Poing : Franzis Verlag, 2002. – 316 S. : mit 83 Abb. – ISBN 3-7723-6345-8

Weber: World Wild West, 2000

WEBER, D.: World Wild West : Polizei und Justiz verstärken den Kampf gegen „Cybercrime“. – In: Neue Zürcher Zeitung. – Internationale Ausgabe. – 2000-05-05, Nr. 104. – S. 49

Winistörfer: Jagd nach Millionen, 1995

WINISTÖRFER, NORBERT: Die verbissene Jagd nach den Millionen. – In: Beobachter. – 1995-03-17, Nr. 6. – S. 18-21

Wolf: Farbe des Geldes, 2000

WOLF, FRITZ: Die Farbe des Geldes : „Gesucht wird.... die Nigeria Connection. Schmutzige Geschäfte mit schwarzen Dollars“. – In: epd medien. – 2000-04-08, Nr. 28. – S. 27

Zietan: Millionen-Einbahnstraße, 2002

ZIETAN, URS: Nigeria-Connection : Millionen auf der Einbahnstrasse. -- In: Spiegel Online. -- URL: <http://www.spiegel.de/netzwelt/netzkultur/0,1518,186621,00.html>. – Zugriff am 2002-05-21

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Diplomarbeit selbständig angefertigt habe. Es wurden nur die in der Arbeit ausdrücklich benannten Quellen und Hilfsmittel benutzt. Wörtlich oder sinngemäß übernommenes Gedankengut habe ich als solches kenntlich gemacht.

Ort, Datum

Unterschrift